Your Guide to Industrial Wireless

www.moxa.com

MOXA®

Preface

Wireless technologies have become increasingly popular in industrial automation as growing numbers of system integrators, governmental agencies, and industrial solution providers continue to turn to these solutions for their applications.

Advantages of using wireless technologies include boosting data transmission speed, real-time data transmissions, remote equipment monitoring and alerts, flexible installation of remote equipment, and wide coverage areas. In addition, wireless technologies can penetrate areas where cables are unable to reach, saving wiring costs. By adopting wireless technologies, industrial applications are able to benefit from greater versatility.

However, the completeness of data, security of transmission, and reliability of the wireless network are constant concerns as wireless technologies rely completely on the emission of electromagnetic waves through the air. Drawing from over 20 years of experience, Moxa offers users the most reliable industrial networking solutions including Turbo Roaming™ for seamless wireless communication, as well as extended wireless transmission ranges of over 10 km. In addition, our complete selection of products for demanding industrial environments includes wide temperature (-40 to 75°C) models, IP67-rated protection from water and dust, and EN50155 certification for rail traffic applications.

We hope this guidebook will provide you with a more comprehensive understanding of industrial wireless technologies and serve as your best guide to getting un-wired!

It's time to go wireless!

Moxa Inc.

Table of Contents

Chapter 1

Differentiating Between Wireless Technologies

1.1 WWAN vs. WLAN vs. WPAN ----------3

- WWAN (Wireless Wide Area Network)
- WLAN (Wireless Local Area Network)
- WPAN (Wireless Personal Area Network)

1.2 Evolution of Cellular Networks ----------4

- 3G Technologies
- 4G Technologies

1.3 Evolution of IEEE 802.11 ----------7

- IEEE 802.11n
- IEEE 802.11s

1.4 WLAN vs. Proprietary 2.4 GHz ----------9

Chapter 2

Understanding Industrial WLAN – IEEE 802.11

2.1 IEEE 802.11 Basics---------- 10

- Electromagnetic Waves
- Signal Power
- Bandwidth, Data Rate, and Throughput

2.2 Wireless Security ---------- 18

- A Peek at the Technology
- The Evolution of Wireless Encryption
- Using a Firewall as an Additional Safeguard

2.3 Antenna Theory and Selection---------- 21

- Functions of Antennas
- Types of Antenna
- Key Antenna Specifications
- Choosing the Right Antenna for Your Project

2.4 Long Distance Wireless---------- 23

- Application Topology
- Components of the Expanded 802.11 Wireless System

Moxa's Antennas Selection Guide ---------- 30

- IEEE 802.11b/g 2.4 GHz Wireless Antennas
- IEEE 802.11a/b/g 2.4/5 GHz Dual-band Antennas
- IEEE 802.11a 5 GHz Wireless Antennas
- Cellular Antennas
- Setting Up Point-to-Point Connections
- Antenna Alignment for P2P Operations
- Moxa Performance Test Report

2.5 Mobile Optimization ---------- 35

- Roaming Under Linear Movement
- Roaming Speed Acceleration
- Limitations of High Speed Roaming

2.6 Advanced WLAN Technologies ---------- 37

- Dual RF Redundancy
- Mesh Technologies
- Wireless VLAN
- QoS for Video/Audio and Control
- Wireless Management

2.7 Industrial Certification---------- 42

- EN50155 Certification
- ATEX/Class I Division 2

Chapter 3

Cellular Networks

3.1 Cellular Basics---------- 44

- Data Service of GSM
- APN in Packet Switch

3.2 Private IP Solution ---------- 48

- Private IP vs. Public IP
- Delay Time
- Solution for Private IP
- Moxa OnCell Central Manager

3.3 Security---------- 50

- The Virtual Private Network (VPN)
- Firewall

3.4 How to Connect Serial Devices to Cellular Networks---------- 51

- Traditional Modems
- IP Gateways

3.5 How to Connect Ethernet Devices to Cellular Networks---------- 56

- From WAN to LAN (TCP Server)
- From LAN to WAN
- The OnCell can be both TCP Server and TCP Client

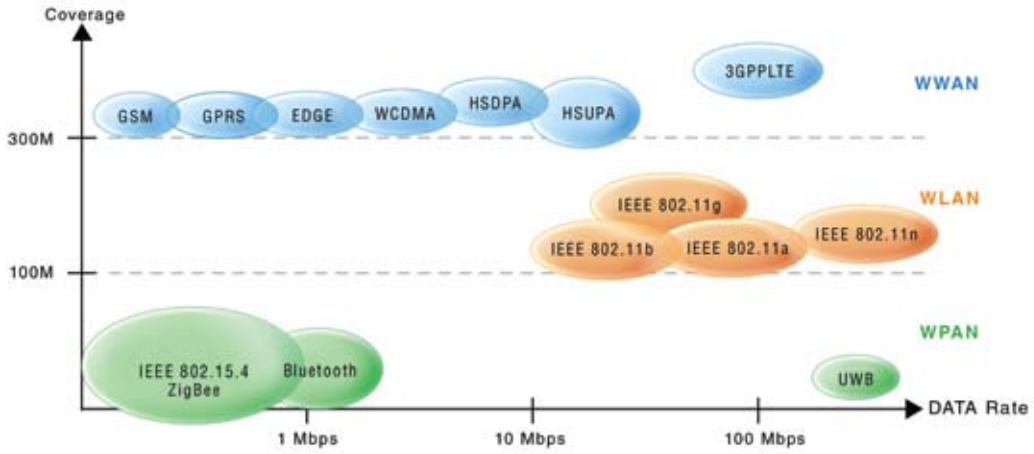
3.6 How to Connect I/O Devices to Cellular Networks ---------- 59

- SCADA Meets Ethernet
- Communication from I/O to SCADA
- OPC Fundamentals
- OPC and DCOM: 5 Things You Need to Know
- Enhance OPC Capability for Cellular Communications
- Conclusion

Chapter 1
Differentiating Between Wireless Technologies

1.1 WWAN vs. WLAN vs. WPAN

Modem wireless technologies are developed for the growing demand in mobile data exchange. Since demands vary depending on the application, different technologies are applied to meet specific needs. Normally, wireless technologies are divided into three categories: WWAN, WLAN and WPAN.



WWAN (Wireless Wide Area Network)

A WWAN utilizes mobile cellular communication networks such as cellular, UMTS, GPRS, CDMA2000, GSM, CDPD, Mobitex, HSDPA, 3G, and WiMax. All of these networks offer wide service coverage and are normally used for citywide, nationwide, or even global digital data exchange. Cellular networks in particular are operated by carriers such as Cingular Wireless, Vodafone, and Verizon Wireless. In cellular communication, GSM (Global System for Mobile Communication) is the leader with over 80% market share, followed by CDMA (Code Division Multiple Access).

The biggest issues regarding data exchange over a WWAN are the associated costs, bandwidth, and IP management. However, as technologies improve and costs drop, WWAN is predicted to replace traditional microwave, RF (radio frequency), and satellite communication due to its lower infrastructure costs.

NOTE: The term “cellular” is also used to refer WWAN technology in general. WWAN technologies are discussed in detail Chapter 3.

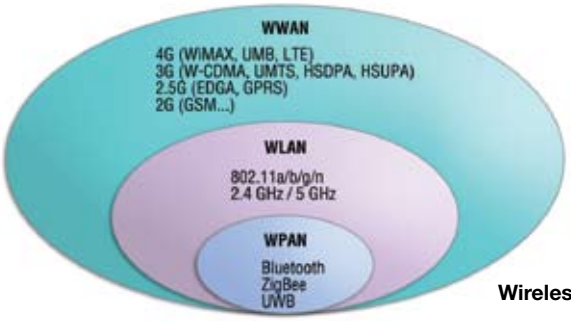
WLAN (Wireless Local Area Network)

As suggested by its name, WLAN transmits data over a shorter distance, normally 100 meters or so. In terms of transmission technology, WLAN uses spread-spectrum or OFDM (Orthogonal frequency-division multiplexing) modulation technology to provide the convenience of exchanging data without the limitation of cables.

Today’s WLANs are based on IEEE 802.11 standards and are referred to as Wi-Fi networks. The 802.11b standard, which operates around the 2.4 GHz frequency band at 11 Mbps, was the first commercialized wireless technology. Advances in wireless technology have made a higher transmission rate of 54 Mbps possible with 802.11g, which also operates around 2.4 GHz, and 802.11a, which operates around the 5 GHz frequency band. It is now very common to see dual-band Wi-Fi access points and client network adaptors that support a mixture of 802.11a, b, and g standards. More bandwidth means that it is possible to use wireless to replace traditional wired solutions to transmit larger data such as video.
NOTE: WLAN technologies are discussed in detail Chapter 2.

WPAN (Wireless Personal Area Network)

A WPAN is a short-range peer-to-peer or ad hoc network built around a person's working area. Normally the distance is no more than 10 meters. Because of their limited transmission range, WPANs are used mainly as cable replacement solutions for data synchronization and data transmission for personal electronic devices such as PDAs or smart phones. Bluetooth is the most prevalent WPAN technology in use today. It allows devices such as phones, mice, headsets, and other personal devices to connect wirelessly within a range of 10 meters. The shorter communication distances also mean lower power consumption, making Bluetooth an even more ideal solution for short-range data transmission. Moxa will be releasing WPAN products in 2010.



Wireless Network Coverage

1.2 Evolution of Cellular Networks

3G Technologies

3G refers to the third generation of telecommunication technologies that is designed to replace 2.5G (GPRS or CDMA). The demand for 3G comes from the growing need for data transmission over wireless networks. The features of cellular networks make them particularly attractive to wireless users in comparison to IEEE 802.11 standards. Cellular has the advantages of wider coverage and the ability to stay connected in high-speed movement. To satisfy the need for data exchange over cellular networks, 3G networks were developed to improve spectral efficiency. The improvements incorporate voice, video, and broadband wireless data transmission all in the mobile environment.

The most commonly seen 3G systems are the Universal Mobile Telecommunication Systems (UMTS) and the Wideband Code Division Multiple Access (WCDMA). These 3G systems are the major revenue contributors to carriers in the past three to two years. As the technologies continue to evolve, transmission speeds have become faster. For example, High Speed Packet Access (HSPA) offers downlink speeds that can reach 144 Mbps and 5.8 Mbps for the uplink. It is not wonder the building of 3G facilities and networks are on the rise. Worldwide subscribers are expected to increase rapidly over the next 3 to 4 years. However, 4G technologies are already in the works and aim to take mobile data transmission to an even higher level.

HSDPA

High Speed Downlink Packet Access (HSDPA), or 3.5G, is a mobile telephony communications protocol. It provides packet data service in WCDMA downlink. The transmission speed can reach 8–10 Mbps on a 5 MHz carrier wave, and 20 Mbps with MIMO technology. In practice, the technologies deployed include AMC, MIMO, HARQ, fast scheduling and fast cell selection.

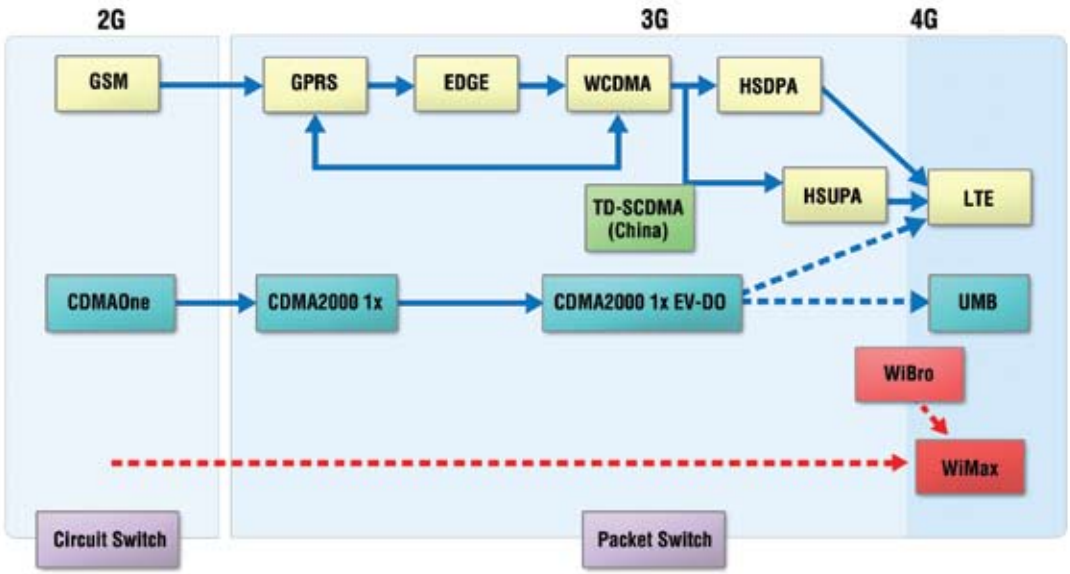
HSUPA

High Speed Uplink Packet Access (HSUPA), or 3.75G, was developed in response to the inadequate upload speed of HSDPA (only 384 Kbps). The transmission speed can reach 10–15 Mbps on a 5MHz carrier wave, 28 Mbps with MIMO technology. The upload speed goes up to 5.76 Mbps, 11.5 Mbps with 3GPP Rel7 technology. With HSUPA, functions requiring massive upload bandwidth (e.g., two-way live transmission or VoIP) can be realized.

CDMA2000 1xEV (Evolution)

CDMA2000 1xEV is CDMA2000 1x equipped with HDR. 1xEV, in general, has two sessions:

- CDMA2000 1xEV 1st session—CDMA2000 1xEV-DO, in light of the fast data transmitted under a wireless channel, supports downlink data speeds up to 3.1 Mbps with uplink up to 1.8 Mbps.
- CDMA2000 1xEV 2nd session—CDMA2000 1xEV-DV (Evolution-Data and Voice) supports downlink data speeds up to 3.1 Mbps with uplink up to 1.8 Mbps. 1xEV-DV also supports 1x voice subscribers, 1xRTT data subscribers, and high speed 1xEV-DV data subscribers to use the same wireless channel at the same time.



4G Technologies

Fourth generation technologies made their market debut in 2009. The goal of 4G is to increase downlink speed to 100 Mbps and uplink speed to 50 Mbps. The two major competing technologies in the 4G market are Long Term Evolution (LTE) and WiMax sponsored by the IEEE Group.

Possible 4G Standards

WiMAX (Worldwide Interoperability for Microwave Access): Led by Intel Corporation, this is the 4G technology with the farthest transmission range. Its highest downlink and uplink speed under mobile communication environments can reach 75 Mbps and 50 Mbps respectively. On November 12, 2008, HTC and Russian carrier Scartel (branded Yota) jointly launched the world's first GSM-WiMAX integrated dual-module mobile phone—HTC Max 4G.

UMB (Ultra Mobile Broadband): Led by Qualcomm Inc., this is the evolution standard of CDMA technology. It has the highest transmission speed among 4G technologies currently. The highest downlink and uplink speed under mobile communication environments can reach 288 Mbps and 75 Mbps respectively.

LTE (Long Term Evolution): LTE is led by ETSI. Its highest downlink and uplink speed under mobile communication environments can reach 100 Mbps and 50 Mbps respectively.

In December 2008, the Third Generation Partnership Project, also known as 3GPP, announced 3GPP Release 8 to enhance data transmission speed in mobile networks. Release 8 standardizes the LTE and makes it a more viable candidate for the nascent 4G standard. LTE uses both Frequency Division Depex (FDD) and Time Division Duplex (TDD), and is able to operate on different bands ranging from 700 MHz to 2.6 GHz. This also makes it possible to incorporate the now incompatible GSM and WCDMA and also reduces costs.

Despite WiMax's current lead in commercializing its technologies, there are signs indicating that LTE is catching up. In the past, major players like Nokia, Siemens, Motorola, Alcatel, Lucent, and Nortel showed their support for WiMax. But starting from 2008, these players were also showing signs of interests in LTE. Nortel had announced not to take part in Mobile WiMax. Alcatel, Lucent, and Motorola also started to discuss LTE, announcing they will take part in both WiMax and LTE development. This has been interpreted as an indication that WiMax development has fallen short of their expectations.

The turning point came with the abandonment of Ultra Mobile Broadband, UMB. When the leading mobile chip provider Qualcomm announced that it will not to invest in UMB but in LTE instead, the CDMA camp also decided to adopt LTE as its standard for next generation technologies. The unification of both CDMA and GSM in LTE gives LTE a great advantage over WiMax.

However, LTE is not expected to dominate the market any time soon. This is because current 3G technologies have raised HSPA+ downlink speed to 42 Mbps. With 100 Mbps possible in the near future with HSPA, LTE will need to offer even more incentives to operators in order for it to become the industry standard.

4G Status

With respect to integration, 4G technologies involve more participants, technologies, industries, and applications than just telecommunications. It can, therefore, be applied to finance, medicine, education, transportation, and other industries. This is because the communication terminal is able to manage more tasks, such as multimedia communications, remote control, and voice communications. If area networks, Internet, telecommunications, radio broadcasts, and satellites are grouped together as an integrated network in the future regardless of the terminal used, they will be able to offer complete wireless and broadband connectivity and higher quality service. Such advancement would allow 4G technologies to penetrate every aspect of our lives.

From the subscribers' perspective, 4G is able to provide faster speed and satisfy more needs. The fundamental driving force of moving mobile communications from analog to digitalization and from 2G to 4G is the shift from wireless voice service to wireless multimedia service in subscriber needs. This has spurred operators to adapt because they need to boost ARPU, develop new frequencies to attract more subscribers, design more efficient spectrum use, and cut their operational costs.

In effect, 4G involves two different but overlapping concepts:

- High-speed mobile telephony system with speed as fast as ADSL's bandwidth (10 Mbps or higher). This concept formerly applied to wireless technologies such as Wi-Fi. It is also the vision addressed by the successful 3G system providers presently.
- Pervasive network technology, a more abstract term often defined as wireless technology that is "ubiquitous, ambient, and everywhere," can involve subscribers in the system completely. Wi-Fi or the system implemented in the future may be applied. This concept also includes Smart Radio technology and has higher spectrum use and transmission capability. Moreover, it can also filter and transmit large volumes of information.

Table: 4G Technology Comparison

Technology	LTE	UMB	WiMax
Standards Setting Organization	RTSI	QCom	Intel
Original Tech.	WCDMA	CDMA2000 1xEV-DO	---
Maximum Speed	100Mbps, 50Mbps	288Mbps, 75Mbps	70Mbps, 70Mbps
Wireless Tech.	OFDM/MIMO/SC-FDMA	MIMO/SDMA	MIMO/SOFDMA
Schedule	2008 draft	2009	2008

1.3 Evolution of IEEE 802.11

With the advent and development of local area networks (LAN), IEEE 802.3 has been widely adopted in many different kinds of communication applications. The continued prevalence of wired communication has also contributed to the growing demand for wireless communication. In 1997, IEEE released the IEEE 802.11 standards that define the Physical Layer and Data Link Layer of TCP/IP, allowing communication based on these protocols to be extended and used with greater flexibility. For the Physical Layer, IEEE 802.11 utilizes non-licensed ISM (Industrial, Scientific and Medical) bands that operate between 2.4 GHz and 5 GHz. In order to make wireless communication more prevalent and feasible, there are also task groups within IEEE designated to develop different wireless applications.

IEEE 802.11	2 Mbps, 2.4 GHz band, 1997, MAC/Physical Standard
IEEE 802.11a	54 Mbps, 5 GHz band, 1999, MAC/Physical Standard
IEEE 802.11b	11 Mbps, 2.4 GHz Band, 1999, MAC/Physical Standard
IEEE 802.11c	MAC Layer Bridging to support IEEE802.1D
IEEE 802.11d	Automatic settings for different countries
IEEE 802.11e	Quality of Service (QoS)
IEEE 802.11f	IAPP, Inter-Access Point Protocol, cancelled by IEEE after February, 2006
IEEE 802.11g	54 Mbps, 2.4 GHz Band, 2003, MAC/Physical Standard
IEEE 802.11h	Support more channels on 5GHz spectrum, 2004
IEEE 802.11i	Wireless security, 2004
IEEE 802.11j	Japanese Standard upgrade, 2004
IEEE 802.11l	Reversed
IEEE 802.11m	Maintenance Standard
IEEE 802.11n	Draft now, using MIMO (Multi-input Multi Output) Technology to increase transmission speed to 300–600Mbps
IEEE 802.11 k	Define measurement items and protocol
IEEE 802.11r	Define implementations of WLAN roaming, enables 802.11 able to be applied to mobile and VoIP applications
IEEE 802.11s	Standard for Mesh under standard architecture

IEEE 802.11n

In January 2004, IEEE made an announcement to form a new task force to develop new standards for the IEEE 802.11 standard. The goal of this task force was to allow wireless communication speed to reach a theoretic number of 300 Mbps. Since the theoretic speed of this new standard, now called IEEE 802.11n, needs to reach 300 Mbps, the Physical Layer also needs to support a higher transmission speed that is at least 50 times faster than IEEE 802.11b and 10 times faster than IEEE 802.11g. In addition to enhancing communication speed, IEEE 802.11n also extends the communication distance to satisfy the growing needs of wireless applications. To make this happen, IEEE 802.11n has added more specifications to the MIMO standard that allows IEEE 802.11n to be able to use multiple antennas to increase transmission speed. It also uses Alamouti coding schemes to increase the transmission coverage.

There are two rival camps competing to dominate the IEEE 802.11n Physical Layer architecture: the World-Wide Spectrum Efficiency, which is supported by Broadcom, and TGnSync, supported by Intel and Philips.

IEEE 802.11s

An 802.11s mesh network device is referred to as a mesh station (mesh STA). Mesh STAs form mesh links with one another, over which mesh paths can be established using a routing protocol. 802.11s defines a default mandatory routing protocol, or HWMP, yet allows vendors to operate using alternate protocols. HWMP is inspired by a combination of AODV (RFC 3561[1]) and tree-based routing.

Mesh STAs are individual devices using mesh services to communicate with other devices in the network. They can also collocate with 802.11 Access Points (APs) and provide access to the mesh network to 802.11 stations (STAs), which have broad market availability. Also, mesh STAs can collocate with an 802.11 portal that implements the role of a gateway and provides access to one or more non-802.11 network. In both cases, 802.11s provides a proxy mechanism to provide addressing support for non-mesh 802 devices, allowing end-points to be cognizant of external addresses.

802.11s also includes mechanisms to provide deterministic network access, congestion control, and power saving.

Table: 802.11 Standards and Date Rate

Protocol	Release Date	Spectrum	Max. Speed	Typical Range (indoor)	Typical Range (outdoor)
802.11	1997	2.4–2.5 GHz	2 Mbps	---	---
802.11a	1999	5.15–5.35/5.47–5.725/ 5.725–5.875 GHz	54 Mbps	30 m	---
802.11b	1999	2.4–2.5 GHz	11 Mbps	30 m	100 m
802.11g	2003	2.4–2.5 GHz	54 Mbps	30 m	100 m
802.11n	2008	2.4 GHz or 5 GHz bands	600 Mbps	50 m	125 m

1.4 WLAN vs. Proprietary 2.4GHz

Common usage of the WLAN limits its distance to under 100 meters. Now with Moxa's advanced technologies, it is also possible to extend the distance up to 10 kilometers for multi-point connections or 20 kilometers for point-to-point connections.

The IEEE 802.11 standard is designed for high-speed data transmission. However, it is also vulnerable to outside interferences. This is unacceptable for some industrial applications where the control elements are often involved. It is a basic control requirement that communication must not be interrupted. To meet this requirement, there are some proprietary 2.4GHz band wireless devices that use FHSS spread spectrum technologies to meet the needs for higher noise resistance. In summary, FHSS sacrifices throughputs and communication ranges for more stability.

Table: WLAN vs. Proprietary Wireless

	Moxa	Banner	
Frequency	2.4 GHz (ISM)	900 MHz (license needed)	2.4 GHz (ISM)
Standard	IEEE 802.11	Proprietary	Proprietary
Spread Spectrum	DSSS / OFDM	*a FHSS	FHSS
Throughput	22 Mbps	115200 bps	115200 bps
Distance	10 km	> 10 km	3.2 km
Communication method	Point to multiple points	Point to point	Point to point

*a: FHSS utilizes frequency hopping to avoid signal interference. Bluetooth is one example that uses this technology. In the early days, IEEE 802.11 also used FHSS but has since adopted DSSS (Direct Sequence Spread Spectrum) out of security concerns. 802.11a, 801.11g, and 802.11n adopt OFDM to increase their resistance to external interferences.

About modulation and spread spectrum, please refer to Chapter 2.1

WWAN vs. WLAN vs. WPAN vs. Proprietary RF

Technologies	WWAN	WLAN	WPAN	Proprietary RF
Standard	GSM/GPRS/CDMA/ WCDMA/WiMax	IEEE802.11	Bluetooth/ ZigBee	No Standard
Connection Mode	Point to point (GSM) WAN (GPRS/3G)	LAN (TCP/IP)	Point to point	Point to Point
Communication coverage	5 km to 30 km	100 m to 300 m	Approx. 10m	100 m to 100 km
Security	High	High	Medium	Low (not standard)
Throughput	50 kbps to 100 Mbps	54Mbps (802.11a/g), 600 Mbps (802.11n)	115200 bps	115200 bps to 1 Mbps

Chapter 2
Understanding Industrial WLAN – IEEE 802.11

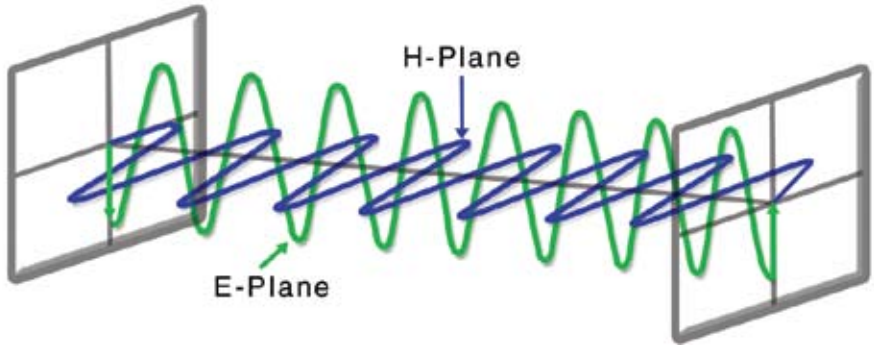
2.1 IEEE 802.11 Basics

Wireless Communication

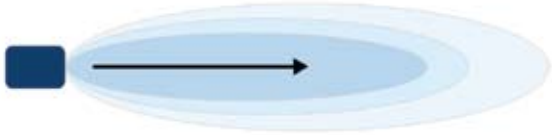
In a wireless environment, the communication medium is air. Radio waves carrying data propagate from point to point through free space. Due to the characteristics of this unguided medium, wireless communication calls for a very different set of knowledge and skills than traditional wired communication systems. Getting the most out of your wireless environment requires a basic understanding of the following scientific principles that govern wireless communications.

Electromagnetic Waves

To understand how energy is transferred through the air, we need to review basic electromagnetic theories. Electromagnetic (EM) waves are formed by alternating current rapidly changing direction on a conductive material. The rapid oscillation of electric and magnetic fields around the conductor projects electromagnetic waves into the air (see the figure below). In order for current to be radiated into the air in the form of electromagnetic waves, a few factors are critical, namely, the length of the conductor and frequency of the AC current. Higher frequency reduces the requirement for conductor length.



The conductors are called antennas. Antennas transform electric energy into EM waves during transmission and turns EM waves into electric energy during reception. The size and length of the antenna is directly proportional to its desired transmission/ reception frequency. As shown in the figure to the right, electromagnetic waves are radiated from a directional antenna in a parabolic shape.



As EM waves propagate through the air, they will experience different types of alterations as they are intercepted by different obstacles. Obstacles in the signal path introduce the following alteration to the signals:

Diffraction (Shadow Fading)

Signal strength is reduced after experiencing diffraction. Obstacles causing diffraction usually possess sharp edges such as the edges of buildings. When EM waves encounter an obstacle with sharp edges that cannot be penetrated, the EM waves wrap around the obstacle to reach the receiver.

Scattering

When EM waves encounter many small obstacles (smaller than wave length), the EM waves scatter into many small reflective waves and damage the main signal, causing low quality or even broken links. Such obstacles include rough surfaces, rocks/sand/dust, tree leaves, street lights, etc.

Reflection

When EM waves run into large obstacles such as the ground, walls, or buildings, they reflect and change their direction and phase. If the reflected surface is smooth, the reflected signal will likely represent the initial signal and not be scattered.

All of the above phenomena results in multipath propagation so not all signals arrive at the receiver antenna at the same time due to obstacles that change the signal paths. Whether you are setting up an outdoor or indoor application, multipath can severely affect received signal quality because the delayed signals are destructive to the main signal. The multipath issue can usually be compensated by antenna diversity at the RF level and/or by OFDM at the baseband level.

Modulation and Spread Spectrum

The following chart categorizes different digital modulation techniques:

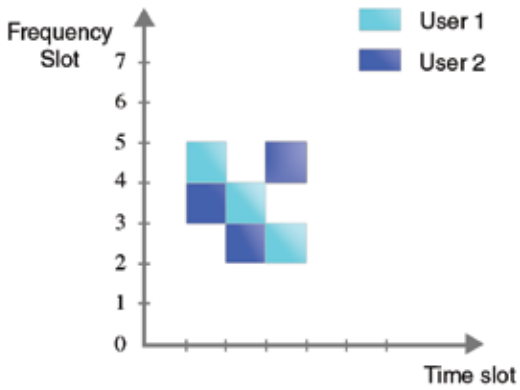
Digital modulation			
linear	**Constant envelope / nonlinear**	**Combined / hybrid**	**Spread spectrum**
BPSK	**BFSK**	**MPSK**	**PN**
DPSK	**MSK**	**M-ary QAM**	**DSSS**
QPSK	**GMSK**	**MFSK**	**FHSS**
$\pi / 4$ **QPSK**		**ODFM**	

As you can see, there are many RF modulation techniques. However, our discussion is limited only to the techniques that pertain to the 802.11 standard, namely FHSS, DSSS, and OFDM.

FHSS (Frequency Hopping Spread Spectrum)

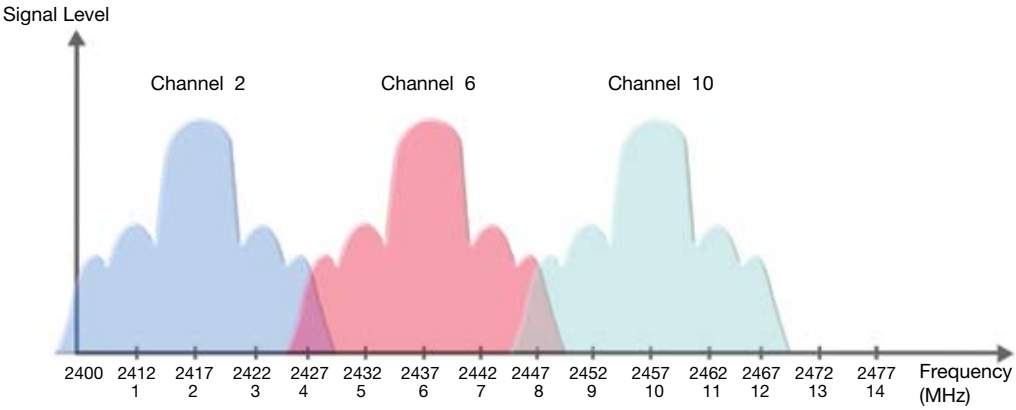
This modulation technique is one of the techniques used in spread spectrum signal transmission. It is also known as Frequency-Hopping Code Division Multiple Access (FH-CDMA). Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal. The transmitter “spreads” the energy, originally concentrated in narrowband, across a number of frequency band channels on a wider electromagnetic spectrum. Some of the advantages include:

- Improved privacy
- Decreased narrowband interference
- Increased signal capacity



DSSS (Direct Sequence Spread Spectrum)

DSSS divides a stream of information to be transmitted into small pieces, each of which is allocated to a frequency channel across the spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. Direct sequence spread spectrum is also known as direct sequence code division multiple access (DS-CDMA). This modulation technique is officially accepted and used by the IEEE 802.11b and IEEE 802.11g standards.



OFDM (Orthogonal Frequency Division Multiplexing)

OFDM is a modulation scheme that divides a single digital signal across 1,000 or more signal carriers simultaneously. The signals are sent at right angles (orthogonal) to each other so they do not interfere with each other. OFDM has the ability to overcome multi-path effects by using multiple carriers to transmit the same signal. OFDM is commonly used in IEEE 802.11a and 802.11g standards. Non/near line-of-sight associations can be achieved using the OFDM technique.

The following table summarizes the modulation techniques:

Modulation Technique	DHSS	FHSS	OFDM
Narrowband Interference	Less resistance (22 MHz wide contiguous bands)	More resistance (79 MHz wide contiguous bands)	Much less (multicarrier modulation)
Interference susceptibility	Medium	High	Low
Collocation	Less	More	Uses several parallel sub-carriers
Compatibility	802.11b (WiFi Alliance)	None	802.11a, 802.11g
Implementation Cost	Comparatively Less	Comparatively more	High
Throughput	5 – 6 Mbps	2 Mbps for 802.11	25 Mbps

Lastly, let's use the 802.11g standard as an example for how the transmission type and modulation scheme corresponds to each data rate:

802.11g Data Rate (Mbps)	Transmission Type	Modulation Scheme
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK1
12	OFDM	*a QPSK
11	DSSS	CCK2
9	OFDM	BPSK3
6	OFDM	BPSK
5.5	DSSS	*b CCK
2	DSSS	QPSK
1	DSSS	*c BPSK

*a QPSK: Quadrature Phase Shift Keying

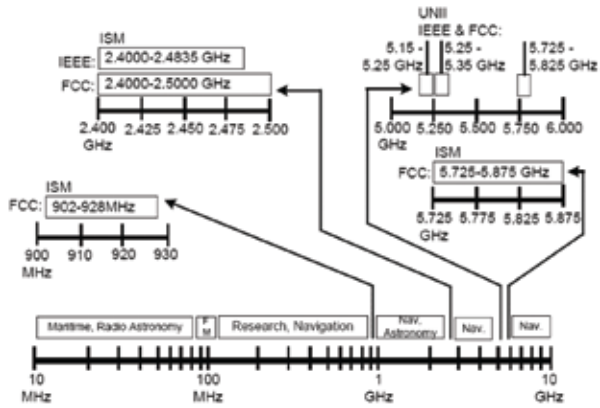
*b CCK: Complementary Code Keying

*c BPSK: Bi-phase Shift Keying

ISM and Licensed Band

The FCC (Federal Communications Commission) regulates the usable frequency bands and the maximum allowable power in these frequency bands for the United States. WLAN devices are allowed to use the ISM (Industrial/Scientific/Medical) band by the FCC. The ISM band consists of 3 different sub-bands: 902 MHz, 2.4 GHz and 5.8 GHz. The FCC has also further defined the UNII (Unlicensed National Information Infrastructure) band for WLAN usage. The following diagram shows the spectrum overview of the ISM and UNII bands.

Figure: ISM and UMI Bands



Advantages and Disadvantages of Using Unlicensed Bands

ISM and UNII are both un-licensed bands which means anyone can transmit in these bands without a license from the FCC. It is the opening of these un-licensed bands that has allowed the WLAN business to grow in small businesses and homes. The freedom of these license-free bands also means a great number of un-licensed users may share the bandwidth with you.

Our discussion only includes the 2.4 GHz ISM band and 5 GHz UNII band because these 2 frequency bands are the most commonly used in WLAN applications.

2.4 GHz ISM Band

As 802.11b/g is the most commonly used WLAN standard today, the 2.4 GHz ISM band is supported by almost every country worldwide. Not every country supports the same channels in the 2.4 GHz ISM band, so you need to make sure the wireless AP matches the standard used by your country. The following chart shows channels supported in the 2.4 GHz ISM band for different countries/continents.

Channel Number	Center Frequency	USA	EU, M. East, Asia	Japan
1	2.412	Y	Y	Y
2	2.417	Y	Y	Y
3	2.422	Y	Y	Y
4	2.427	Y	Y	Y
5	2.432	Y	Y	Y
6	2.437	Y	Y	Y
7	2.442	Y	Y	Y
8	2.447	Y	Y	Y
9	2.452	Y	Y	Y
10	2.457	Y	Y	Y
11	2.462	Y	Y	Y
12	2.462		Y	Y
13	2.472		Y	Y
14	2.484			Y *DSSS only

The FCC opened the frequency band between 2.4 to 2.5 GHz, and the IEEE uses 2.400 to 2.4835 GHz. The minor mismatch is to provide a buffer to prevent power from leaking into the forbidden band.

UNII Band

The 5 GHz UNII band consists of 3 parts, each 100 MHz wide. The 802.11a standard uses this band. Each part of the UNII band includes 4 non-overlapping channels with 5 MHz of guard band between them. The FCC states that the lower band (UNII-1) can only be used indoors, the middle band (UNII-2) can be used indoors or outdoors, and the higher band (UNII-3) should only be used outdoors. Since UNII-1 and UNII-2 can be used indoors, the maximum number of non-overlapping channels in an indoor environment is 8. See below for channels supported in the 5 GHz UNII band for different countries.

Channel ID	Frequency (MHz)	USA	EU, M. East, Asia	Japan
36	5180	V	V	V
40	5200	V	V	V
44	5220	V	V	V
48	5240	V	V	V
52	5260	V	V	V
56	5280	V	V	V
60	5300	V	V	V
64	5320	V	V	V
100	5500	V	V	V
104	5520	V	V	V
108	5540	V	V	V
112	5560	V	V	V
116	5580	V	V	V
120	5600	V	V	V
124	5620	V	V	V
128	5640	V	V	V
132	5660	V	V	V
136	5680	V	V	V
140	5700	V	V	V
149	5745	V		
153	5765	V		
157	5785	V		
161	5805	V		
165	5825	V		

Signal Power

Radio signals are transmitted with a certain power level. Power is measured in watts. However, a watt is a rather large amount of power in WLAN. Therefore, power is usually measured in milliwatts (mW), which is one-thousandth of a watt. A typical wireless AP transmits between 30 to 100 mW of power, and about 50 mW for wireless adaptors (clients). Certain applications will require higher transmit (Tx) power and may attempt to use power boosters or customized high power modules to amplify the transmit power. However, such attempts may cause the system to exceed the radio emission regulations (i.e., FCC regulations) of one's country so take caution during high power operation.

dB, dBm, dBi

Power measured in mW is hard on the math when we are dealing with extremely small power levels at the receiver end. Therefore, instead of using absolute values (milliwatts) we often convert them into dBm. The unit of dBm is a logarithmic representation of mW. The conversions are as follows:

$$P_{dBm} = 10 \log P_{mW}$$

$$P_{mW} = \log^{-1}\left(\frac{P_{dBm}}{10}\right)$$

The following table shows some common conversion values between dBm and mW:

dBm	Watt	dBm	Watt
+40dBm	10W	+12dBm	16mW
+30dBm	1W	+9dBm	8mW
+20dBm	100mW	+6dBm	4mW
+10dBm	10mW	+3dBm	2mW
0dBm	1mW	0dBm	1mW
-10dBm	100uW	-3dBm	500uW
-20dBm	10uW	-6dBm	250uW
-30dBm	1uW	-9dBm	125uW
-40dBm	100nW	-12dBm	62.5uW

The dB is a unit of relative quantity, which means it is merely a multiplication factor used to represent the gain or loss of signal power. A useful rule of thumb is an addition or subtraction of 3 dB is equivalent to a multiple of 2 or 0.5. An addition or subtraction of 10 dB is equivalent to a multiple of 10 or 0.1.

In dealing with antenna gain specifications, the gain factor is often represented by "dBi". The "i" stands for "isotropic", which means the gain is relative to an isotropic radiator (i.e., a radiating sphere in space). This ideal radiation is impossible to realize but its pattern is the reference for all realizable antennas. The gain of a passive antenna is measured by how effectively the antennas can focus the energy (how narrow is the antenna angle), rather than the actual boost in transition power. Therefore, the narrower the antenna angle, the higher the antenna gain. The diagram below shows the antenna angles of a high and low gain antenna.

Low Gain Antenna

High Gain Antenna

Transmit Power and Received Sensitivity

When a radio signal is being transmitted through the air, it will experience a great loss in signal strength caused by attenuation introduced by free space. Therefore, when evaluating a wireless system, one needs to be aware of the signal power level at the transmitter end and at the receiver end. The signal power received cannot be so weak as to break the communication link, or too strong as to saturate the receiver's amplifiers.

These concerns call for estimating the "power budget" of a wireless system. By making a power budget estimation, you will have an idea of how far you can extend your wireless link without losing communication. Please note that the following calculations are pure theoretical estimations that are not meant to guarantee communication distance. There are many other factors involved that will affect transmission distance.

$$\frac{P_r}{P_r} = \frac{G_t G_r}{f_L}\left(\frac{\lambda}{4\pi d}\right)^2 \qquad d = \frac{10^{(Pt + Gt + Gr - Pr)/20}}{41.88 \times f}$$

Pt : Transmit Power
Gt, Gr: Antenna Gain
Pr: Sensitivity

f is the frequency in mHz, pt and pr in dBm, and gt and gr in dBi, which are easier to obtain from product specifications. To get the effective range d in km, all we have to do is plug in the values for pt, pr, gt, gr, and f.

The receiver's sensitivity is the minimum power level the receiver can accept to process the received data. The specified sensitivity is not the power detected by the receiving antenna but the power present as the receiver module. An important point to note from the above equation is that as frequency increases, the effective distance decreases. Therefore, the 802.11a (5 GHz) standard will yield a shorter communication distance than 802.11b/g (2.4 GHz). Users who wish to communicate long distances should therefore select 802.11b/g as their operating standard.

Bandwidth, Data Rate, and Throughput

Usually when "bandwidth" is mentioned, it means one of two things:

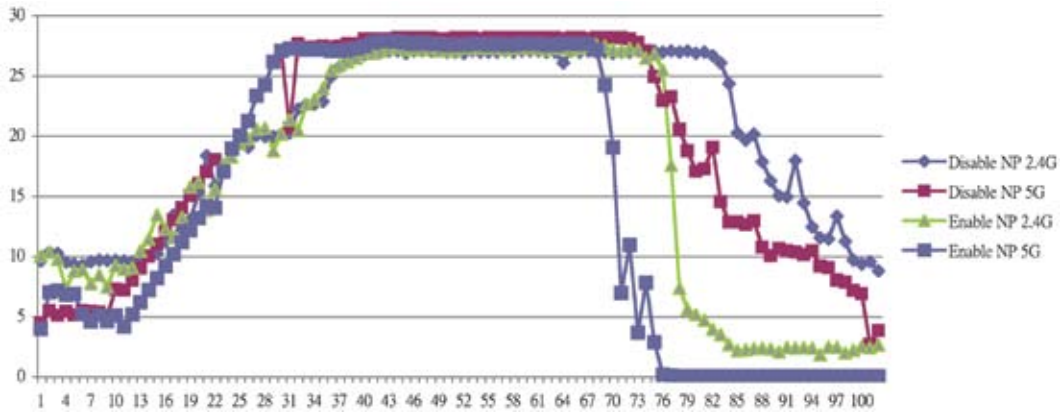
1. The actual width of a frequency band measured in Hz (Hertz); the effective bandwidth would be the frequency band that is actually carrying data.

2. The maximum data rate available (bits per second) in a communication link.

The former is the technically correct definition of bandwidth. For example, the 802.11b/g standards operate between 2.4 GHz and 2.4835 GHz, giving a total effective bandwidth of 83.5 MHz with a channel bandwidth of 22 MHz.

The data rate of a particular wireless standard is the maximum data transfer speed (bit per second) the communication link can achieve, such as 54 Mbps for 802.11g. Please note that this is the specified transfer rate for raw data. The WLAN protocol packages the user data with layers of headers and trailers with inter-packet gaps in between the packets. For example, TCP communication requires the receiving end to acknowledge the received data by sending ACK packets back to the receiver. Therefore, the actual user data rate will be lower than the specified data rate because user data is only a portion of the raw data being transmitted via the wireless media. The actual user data rate is called the "throughput" of the wireless link. Typically, we can expect the throughput to be about half of the specified data rate (i.e., throughput = 25 Mbps when data rate = 54 Mbps).

The following figure is an example of throughput measurements as signal attenuation increases (curves correspond to different noise immunity settings):



As you can see, when the signal is too strong (low attenuation) or too weak (high attenuation), the overall throughput dips bellow the optimum value.

Throughput can be measured with various throughput measuring tools. One of the free throughput measuring tools available is Jperf, downloadable here: http://sourceforge.net/projects/iperf

2.2 Wireless Security

If you're new to wireless, the first thing you should realize is that the signals you send and receive from a nearby access point are easily intercepted by anyone in the vicinity who has a wireless card and a computer. The purpose of WLAN security techniques is to render the connection unusable and the data unreadable by anyone but you and the person (or machine) you're communicating with.

Although most people do not need in-depth knowledge of WLAN security, understanding the basics can make it easier for you to find the right product for your application. For example, one of the most basic questions you can ask is whether or not a product supports WPA and/or WPA2. But why should you care? Most wireless products available on the market today support WEP. Even though WEP may protect your data from the casual passerby, it still leaves you vulnerable to attack from someone with some basic network knowledge and some time on their hands, as we point out in the next section.

A Peek at the Technology

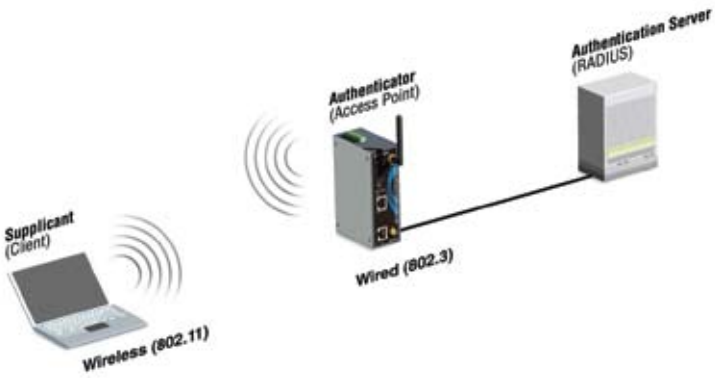
There are two basic aspects to wireless security: authentication and encryption. Simply put, a system uses authentication to check a user's credentials and determine if the user should be given access to the data and resources provided by the protected network. Encryption, on the other hand, encodes the data so that anyone who does not have the secret "key" will not be able to read the data.

Authentication

The 802.1X standard dictates how authentication on wired and wireless LANs is carried out. 802.1X authentication uses port-based access control, which means that the various entities involved in the authentication process gain access to each other's resources by connecting through "ports." In effect, the authentication procedure involves placing a "guard" at each port to prevent unauthorized users from gaining access to protected data.

The 802.1X authentication procedure involves three basic players:

- The supplicant is the client (PC or laptop computer, for example) who would like to gain access to network resources through the wireless network.
- The authenticator, which is usually an access point (AP) for a wireless network, plays the role of gatekeeper.
- The authentication server, which connects to the AP over a wired network, handles the authentication procedure. More often than not, a RADIUS server is used.



In effect, the authenticator and authentication server work as a team to verify the identity of the supplicant. The authentication server also takes responsibility for computing the "keys" that the encryption algorithm will use. Although the details of authentication may be complex, the overall procedure is easy to describe:

STEP 1: The Authenticator relays authentication messages between the WLAN and the Ethernet.

STEP 2: The Authentication Server and Supplicant establish a secure tunnel that is used to pass encrypted messages.

STEP 3: The Authenticator performs the authentication check based on the agreed upon method (TLS, PEAP-MSCHAP-V2, TTL, etc.).

Encryption

The science of encryption or, in more down-to-earth terms, the making and breaking of codes, is one of the most crucial aspects of WLAN technology. This is because the radio waves used to transmit data packets between your computer and the wireless access point can pass through walls, floors, and other barriers. People who use laptops that have a wireless LAN card will know this first-hand, since it is often possible to pick up signals from wireless access points located in nearby apartments. Using a password to restrict entry to your network may not provide enough protection, since a reasonably clever person can still intercept your data packets. In fact, if the person intercepting the wireless data is more than reasonably clever, he or she may also be able to download and read the contents of the packets.

As illustrated in the schematic below, wireless encryption has evolved from WEP, which was released in 1999, to the 802.11i standard, more commonly referred to as WPA2.

The Evolution of Wireless Encryption

WPA2

WPA2 is the second generation of WPA. The primary difference between WPA and WPA2 is the technology used for data encryption. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption, whereas WPA2 uses Advanced Encryption Standard (AES), a stronger encryption technology suitable for industries that require highly secure networks.

WPA

Wi-Fi Protected Access (WPA) is a stronger security method that was created in response to the flaws discovered in WEP. It was intended as an intermediate measure until further 802.11i security measures were developed. When implemented with authentication methods such as RADIUS, WPA is considered secure enough for all but the most sensitive enterprise applications. For most home and small business use, an effective level of security can be obtained by using WPA with a pre-shared key (PSK) that is shared by all users.

802.1X

802.1X is an authentication method that prevents unauthorized users from entering the network. It is used with WPA to form a complete WLAN security system. On many wireless systems, users either log into individual access points, or can freely enter the wireless network but cannot get further without additional authentication. 802.1X makes users authenticate to the wireless network itself, not an individual AP or another other level like a VPN. This is more secure, as unauthorized traffic can be denied right at the AP.

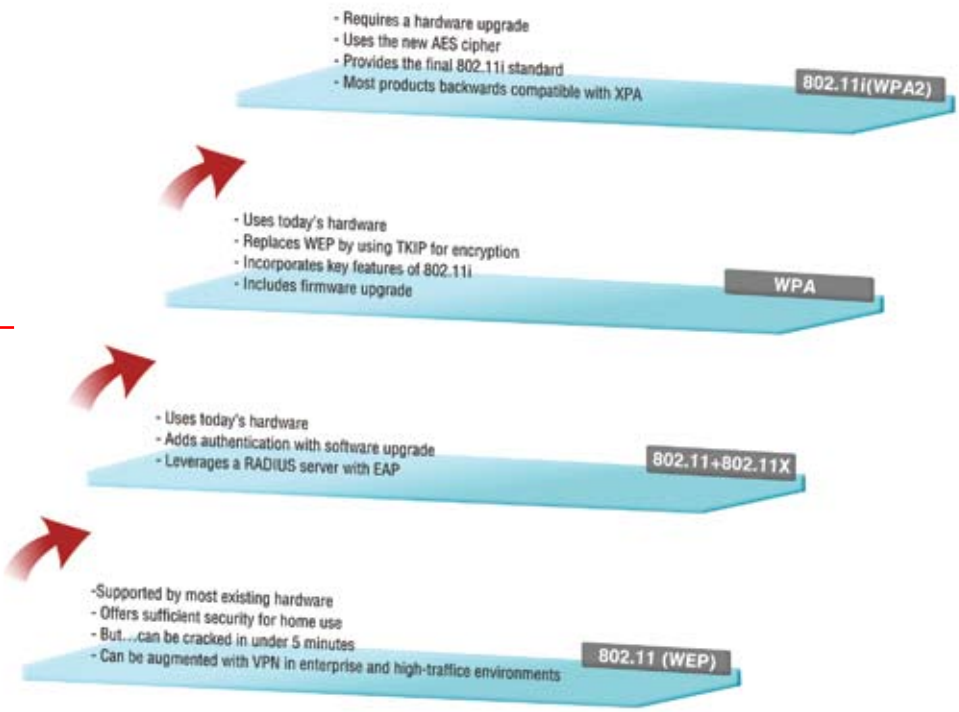
WEP

Wired Equivalent Privacy (WEP) provides a basic level of security to prevent unauthorized access to the network and protect wireless data. Static shared keys (fixed length alphanumeric/hexadecimal strings) are used to encrypt data and are manually distributed to all wireless stations that want to use the wireless network. WEP has been found to have serious flaws and is not recommended for networks that require a high level of security. For more robust wireless security, most access points support Wi-Fi Protected Access (WPA or WPA2) for improved data encryption and user authentication.

Using a Firewall as an Additional Safeguard

One of the most basic aspects of maintaining the security of your network involves using a firewall to filter out unwanted traffic. To protect a private LAN from unwanted traffic originating outside the LAN, firewall software often runs on a gateway that connects the LAN to the Internet. The firewall is configured to filter out traffic based on various characteristics of the incoming packets, such as IP address, MAC address, type of protocol, etc.

Even if your private LAN does not connect to a public network, once you allow access to the LAN through a wireless AP, you open the network to possible external attack. As an added safeguard, some manufacturers include firewall software on the access point to filter out traffic accessing the network through the AP. For example, Moxa's AWK-3121 supports the latest encryption technology (WEP, WAP, WAP2) and allows system managers to filter traffic by MAC address, IP, as well as TCP/UDP filtering options.


- Requires a hardware upgrade
- Uses the new AES cipher
- Provides the final 802.11i standard
- Most products backwards compatible with XPA
802.11i(WPA2)
- Uses today's hardware
- Replaces WEP by using TKIP for encryption
- Incorporates key features of 802.11i
- Includes firmware upgrade
WPA
- Uses today's hardware
- Adds authentication with software upgrade
- Leverages a RADIUS server with EAP
802.11+802.11X
-Supported by most existing hardware
- Offers sufficient security for home use
- But…can be cracked in under 5 minutes
- Can be augmented with VPN in enterprise and high-traffice environments
802.11 (WEP)

2.3 Antenna Theory and Selection

Choosing the right antenna after a site survey is a small but important factor when planning a wireless project. The purpose of this section is to explain what an antenna is and how to choose the right antenna to help build a reliable wireless network.

Functions of Antennas

An antenna is a transducer that is designed to transmit or receive electromagnetic waves. It is like a converter that converts electromagnetic waves and electrical currents back and forth. Different wireless devices use different antennas to operate in different frequencies and to achieve, for example, a desired range. The most important parameter of an antenna is its working frequency. For example, a 2.4GHz antenna is too weak to use in IEEE 802.11a communication and the data rate will fall back to a very low level or even drop to ground zero.

Types of Antenna

There are two basic types of antennas, omni-directional and directional. The two types are categorized by the direction in which they beam radio signals. Omni-directional antennas are designed to radiate signals equally in all directions. Use this type of antenna if you need to transmit from a central node, such as an access point, to users scattered all around the area.

Directional antennas provide a more focused signal than omni-directional antennas. Signals are typically transmitted in an oval-shaped pattern with a beam width of only a few degrees. With higher gain, directional antennas can also be used outdoors to extend point-to-point links over a longer transmission distance, or to form a point-to-multipoint network.

Key Antenna Specifications

Connector types

Before you purchase an antenna for your wireless device, you should check the type of antenna connector that your device uses. You will need to buy an antenna with a matching connector. There are several types of antenna connectors, including MCX, TNC, N-type, SMA, and RP-SMA (RP stands for “reverse polarity” or “reverse ping”). On WLAN devices, the most commonly used antenna connector is PRSMA and N-type for IEEE 802.11 wireless applications.

N-type(male) N-type(female) RP-SMA(female) RP-SMA(male) SMA(female) SMA(male)

Half-Power Beam Width (HPBW)

This parameter is measured from the antenna’s radiation pattern, and refers to the beam width at which the antenna’s radiation drops to half of its peak value. It also refers to the antenna’s effective coverage area. Once you get outside the half-power beam width, the signal typically drops off very quickly. A very high-gain antenna has a very narrow angled half-power beam width, which makes the directionality high as well.

Antenna Polarity

Polarization refers to the direction in which the electromagnetic field lines point as energy radiates away from the antenna. The simplest and most common type is linear polarization. When power is sent from transmitter to receiver, only that portion of the beam with the same polarization can be received. An improper antenna installation may decrease performance.

Frequency

Different wireless applications use different frequencies to achieve their purposes. To make sure wireless devices work as expected, users need to choose the right antenna with the right frequency. For example using a 5GHz IEEE 802.11a application with a 2.4GHz antenna can weaken or even completely wipe out the signal.

Choosing the Right Antenna for Your Project

In addition to the key antenna specifications outlined above, there are some very simple tips you can use to choose the right antenna for your wireless project.

For a fixed point-to-point connection, we recommend choosing a directional antenna. Rather than broadcasting their signals linearly, directional antennas form a Fresnel Zone (a spherical expansion of the signal waves) and increase signal strength. The increased signal strength ensures smoother data transmission and connection.

When facing an application that requires constant changing of locations, omni-directional antennas make a better choice. An omni-directional antenna emits waves equally in all directions so it is easier for moving objects with constantly changing angles and positions to receive signals.

A few applications require special types of antennas, such as a leakage antenna for collecting data along rail tracks. These are very special cases and the deployment and infrastructure costs can be very high.

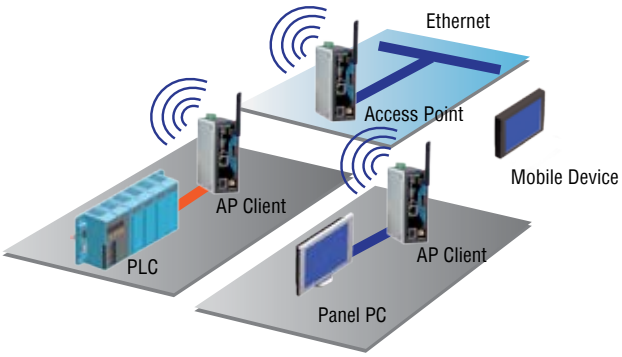
2.4 Long Distance Wireless

Wireless transmissions today are based upon the IEEE 802.11 protocol stacks. By modifying these stacks, wireless solution providers can optimize them for long-range, point-to-point applications. It has also been used in the developing world to link communities separated by difficult geography with little or no connectivity options. In this section, we will introduce long distance wireless technology and list the components required to extend your wireless range.

Application Topology

Wireless Link (AP-Client Mode)

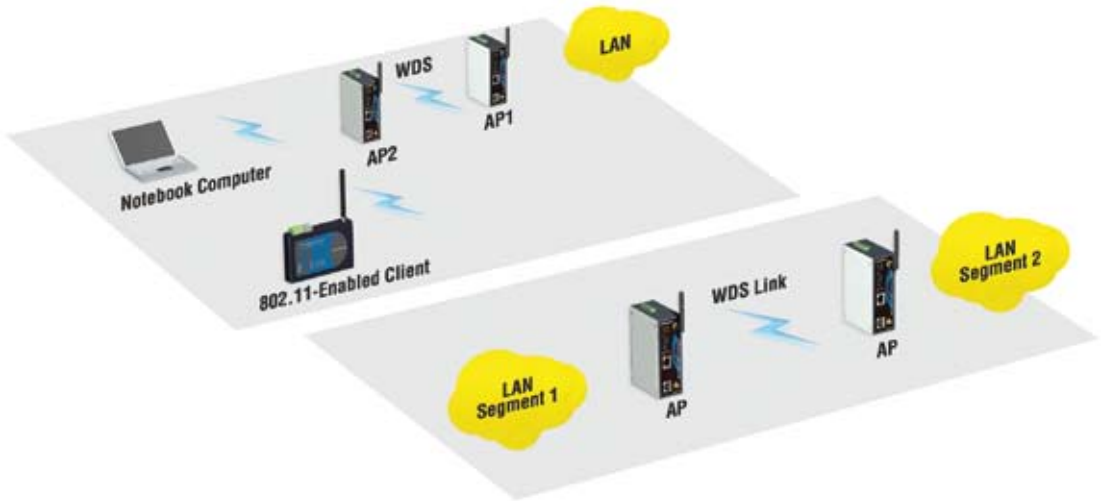
By setting up a wireless link between the AP and Client, several buildings in an extensive corporate campus can be easily integrated into the company network. AP-Client connections can also be used to provide Internet access in areas where cabling would be too expensive or impractical to install. A good LOS (Line of Sight) is required between the AP and Client devices. Distances of several kilometers can be bridged by this type of wireless link.



AP-Client Operation

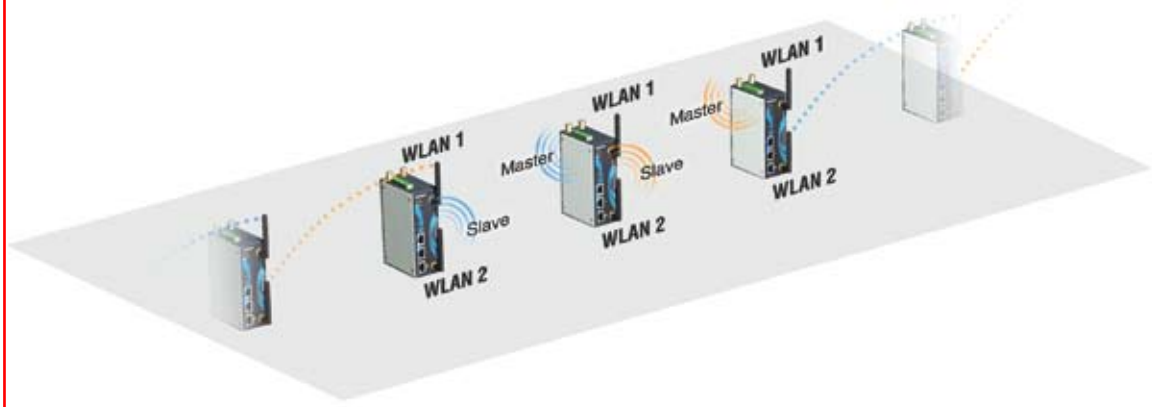
Wireless Distribution System (WDS)

Wireless Distribution System (WDS) is a special type of wireless link. This mode allows several buildings on a company to be connected to the central office. The central AP is configured the partner MAC (Media Access Control) the remote WDS AP is configured the central AP MAC (Media Access Control). The wireless link will reduce half bandwidth (due to use the same frequency channel) when add more one AP under chain connection.



Wireless Bridge System (Dual RF)

Moxa's proprietary Wireless Bridge System (Dual RF) allows several buildings on a corporate campus to be connected to the central office. The central AP is configured as the "master" device and the remote client stations as "slave" devices. The wireless link will not reduce the bandwidth (to due to the use of Dual RF and isolation of the overlap frequency channel) but will extend the wireless range.



Components of the Expanded 802.11 Wireless System

Expanded 802.11 wireless systems consist of the following components, some of which are optional.

Access Points

Moxa supplies 802.11a/b/g/n (802.11n will be implemented in the future, the technology works by using multiple antennas to target one or more sources to increase transmission power and throughput) wireless AP/Bridge/Client devices to extend the wireless range.

IEEE 802.11a is a modified version of the IEEE 802.11 standard and was approved in 1999. IEEE 802.11a adopts the same standards as IEEE 802.11 and operates in the 5 GHz band. It uses 52 Orthogonal Frequency Division Multiplexing (OFDM) waves and has a maximum capacity of 54 Mbps. This has already satisfied the standard requirement of network communication which needs around 20 Mbps of bandwidth. It is also possible to drop the communication speed to 48, 36, 24, 18, 12, 9 or even 6 Mbps. IEEE 802.11a has 12 parallel channels, among them 8 of which are used for indoor communications and 4 for point-to-point communications. IEEE 802.11b is not inter-operable with IEEE 802.11a unless the communication devices support both standards. IEEE 802.11a has the advantage of less interference than IEEE 802.11b as IEEE 802.11b's 2.4 GHz band is widely used. However, the high frequency also has some downsides. IEEE 802.11a has a much narrower coverage, so it needs more access points. This also means that signals can not be transmitted as far as IEEE 802.11b because it is much easier for signals to be absorbed by surrounding objects.

Parameter Tuning

Wireless devices have traditionally been limited in range due to the inherent design of the 802.11 standard. 802.11 protocol uses acknowledge for each received frame. If an acknowledgement is not received, the frame is re-transmitted. By default the maximum distance between transmitter and receiver is 1 mile (1.6 km). On longer distances the delay will force retransmissions so Moxa has tuned our Wireless product to support long-range deployments using wireless 802.11.

Moxa Wireless Products are now enhanced with the ability to automatically adjust parameters such as slot time, ACK time-out, and CTS time-out to fine tune the wireless device for optimal performance and achieve a longer range.

Environmental Conditions:

Two factors are considered as below:

- **2.4GHz interference**: There are literally hundreds of other sources of interference that aggregate into a formidable obstacle to enabling long range use in occupied areas: microwave ovens, baby monitors, wireless cameras, remote car starters, wireless phones, and Bluetooth products.
- **Landscape interface**: Obstacles are among the biggest problems when setting up a long-range wireless application. Trees and forests degrade the microwave signal, and rolling hills make it difficult to establish line-of-sight propagation. In a city, buildings will impact integrity, speed and connectivity. Steel frames partly reflect radio signals, and concrete or plaster walls absorb microwave signals significantly, but sheet metal in walls or roofs may efficiently reflect wireless signals, causing an almost total loss of signal.

Power Amplifier

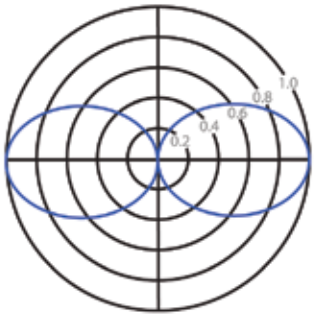
Moxa supplies RF devices with 63/200/800 mW and boosters to extend your wireless range.

For example, if you have a 18 dBm (63 mW) device and replace Moxa's 200 mW RF device, you can increase 18 dBm (63 mW) to 23 dBm (200 mW); if you replace Moxa's 800 mW RF device, you can increase 18 dBm (63 mW) to 29 dBm (800 mW). Based on our experience, you can increase the range by using Moxa's RF devices or boosters.

External Antennas

Moxa's 802.11a/b/g/n wireless AP/bridge/client devices are supplied with a low gain antenna. However, for many of the long range applications, additional external antennas are necessary to extend the wireless range. The following sections contain a brief description of the two types of antennas:

- Omni-directional antennas transmit horizontally with equal power in all directions. They have very limited vertical spread, which determines the antenna gain. Antennas of this type are typically located in the center of open spaces or larger offices to provide even coverage to all clients.



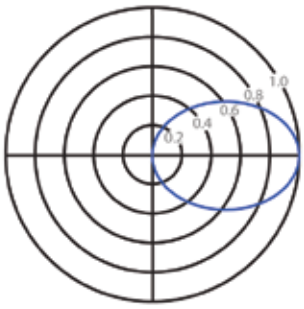
E-Plane

H-Plane

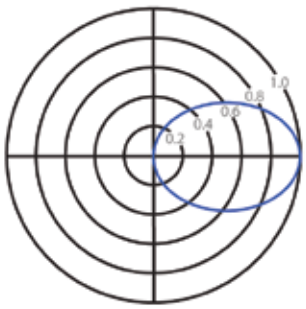
Fiberglass Antenna

Dipole Antenna

- Uni-directional antennas have beams with narrow horizontal and vertical angles. Uni-directional antennas are mainly used on rooftops or masts for establishing point-to-point links that interconnect areas of a network that are separated by a distance.



E-Plane



H-Plane

Directional / Panel Antenna

Setting Up Point-to-Point Connections

This sector introduces the basic principles involved in designing point-to-point links and provides tips on aligning the antennas.

The following basic questions must be answered when designing long range wireless links:

- What antennas are required for the desired application?
- How must the antennas be positioned to ensure a problem-free connection?
- What performance characteristics do the antennas need to ensure sufficient data throughput within the legal limits?

MOXA Antenna Calculator

You can use the Moxa Antenna Calculator to calculate the output power of the access points as well as the achievable distances and data rates. The program can be used from our website at www.moxa.com/Event/IW/2009/Industrial_Wireless_Typology/index.htm

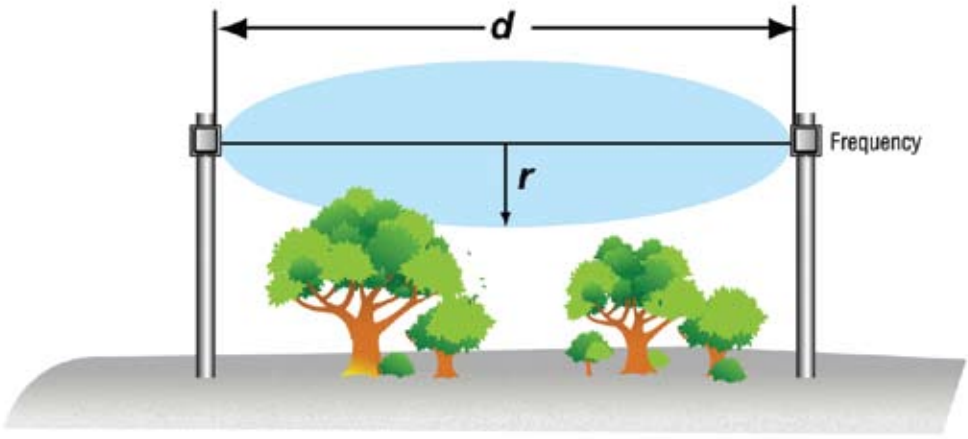
After selecting your components (access points, antennas, cable, etc.) the calculator works out the data rates, ranges, and the antenna gain settings that have to be entered into the access point.

Positioning the Antennas

Antennas do not broadcast their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves results in amplification of or interference to the effective power output at certain intervals of the connection between the transmitter and receiver.

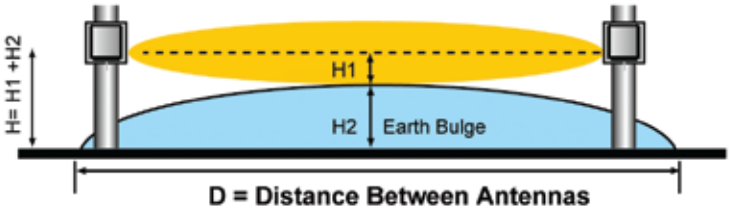
The Fresnel Zone must remain free from obstruction in order to ensure that the maximum level of output from the transmitting antenna reaches the receiving antenna. Any obstructing element protruding into this zone will significantly impair the effective signal power. The object not only screens off a portion of the Fresnel Zone, but the resulting reflections also lead to a significant reduction in signal reception.

The concept of RF LOS is based on a parabolic free space zone called the Fresnel Zone that will ensure a more stable link if at least 60% of the vertical radius is kept obstacle free. The figure below shows how to estimate the Fresnel Zone of a wireless link where **r** (meter) is the vertical radius of the oval, **d** (km) is the distance between the transceivers, and **f** (GHz) is the radio frequency.



$$r_{(In\ mts)} = 17.32X\sqrt{\frac{d_{(In\ km)}}{4f_{(In\ GHz)}}}$$

To ensure that the Fresnel Zone remains unobstructed, the height of the antennas must exceed that of the highest obstruction by this radius. The figure below shows the full height of the antenna mast.



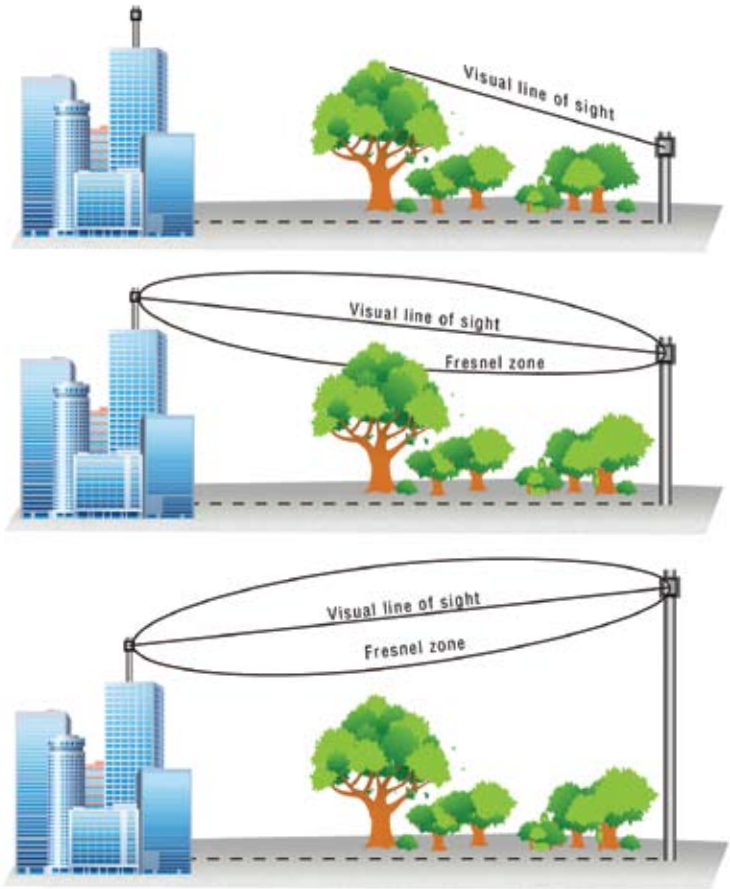
H1 = Added Antennas Height for Fresnel Zone Clearance
H2 = Added Antennas Height for Earth Bulge Clearance

Antenna Gains

The gain of each antenna specifies its directionality. In general, the lower the gain, the more evenly distributed in all directions the radiation will be. High gain antennas, on the other hand, emit radiation in a more specific direction. The gain defines its power gain or directive gain in terms of the ratio of the intensity, or power per unit surface. In general, when we choose an antenna, the longer the transmission distance, the higher the antenna gain must be. At the same time, we must sacrifice omni-directional coverage.

Antenna Alignment for P2P Operations

When there is not enough obstacle-free Fresnel Zone available, you may need to relocate the wireless devices or elevate the antennas to clear more Fresnel Zone space (see figure below). In long distance applications, Earth Bulge may need to be taken into consideration as an obstacle.

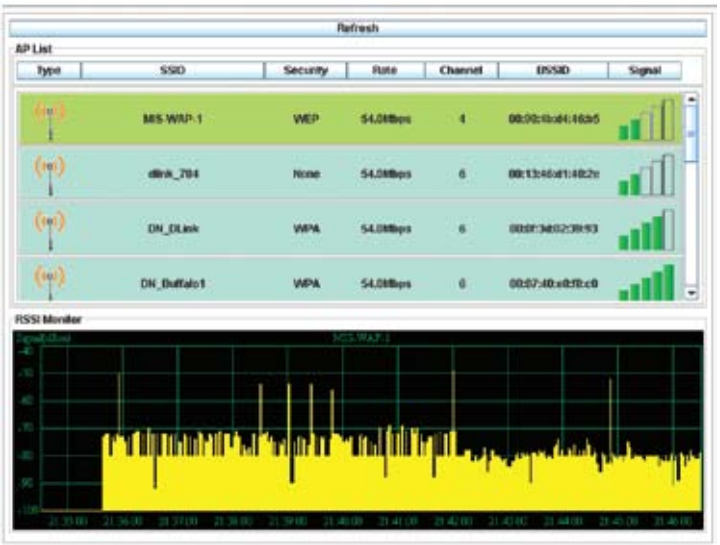


The precise alignment of the antennas is of considerable importance in establishing long range wireless connections. The more central the receiving antenna is located in the “ideal line” of the transmitting antenna, the better the actual performance and the effective bandwidth are. If the receiving antenna is outside of this ideal area, however, significant losses in performance will result.

The current signal quality over a long range wireless connection can be displayed on the device’s LEDs or in the Moxa monitor in order to help find the best possible alignment for the antennas. The more LED indicators means the stronger the connection.

In the Moxa monitor, the connection quality display is opened with the context menu once signal monitoring has commenced. The P2P dialog displays the absolute values for the current signal strength and the maximum value upon starting the measurement. The development of the signal strength over time and the maximum value are displayed.

Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.



Moxa's Antennas Selection Guide

IEEE 802.11b/g 2.4 GHz Wireless Antennas

Product Name	ANT-WSB-AHRM-05-1.5m	ANT-WSB-ANF-09	ANT-WSB-PNF-12	ANT-WSB-PNF-18
Antenna Patterns	E-Plane H-Plane	E-Plane H-Plane	E-Plane H-Plane	E-Plane H-Plane
Frequency Range	2.4 to 2.5 GHz	2.4 to 2.5 GHz	2.4 to 2.5 GHz	2.4 to 2.5 GHz
Antenna Type	λ/4 Dipole	Omni-directional	Directional, Panel	Directional, Panel
Typical Antenna Gain	5 dBi	9 dBi	12 dBi	18 dBi
Impedance	50±5 ohms	50±5 ohms	50±5 ohms	50±5 ohms
Polarization Linear	Vertical	Linear	Linear	Linear
HPBW/ Horizontal	360°	360°	50°	30°
HPBW/Vertical	---	10°	30°	20°
V.S.W.R.	2.0	1 : 1.3 Max.	1 : 1.5 Max.	1 : 1.5 Max.
Power Handling	---	15 W Max.	10 W Max.	15 W Max.
Connector(s)	RP-SMA (male)	N-type (female)	N-type (female)	N-type (female)
Operating Temperature	-40 to 80°C	-40 to 80°C	-40 to 80°C	-40 to 80°C
IP Rating	---	IP65	IP65	IP65
Antenna Profile	---	420 mm length	215 x 90 x 30 mm	270 x 205 x 15 mm
Weight	300 g	430 g	560 g	1020 g

IEEE 802.11a/b/g 2.4/5 GHz Dual-band Antennas

Product Name	ANT-WDB-ANF-0609	ANT-WDB-PNF-1518
Antenna Patterns	E-Plane (2.4 GHz) E-Plane (5 GHz) H-Plane (2.4 GHz) H-Plane (5 GHz)	E-Plane (2.4 GHz) E-Plane (5 GHz) H-Plane (2.4 GHz) H-Plane (5 GHz)
Frequency Range	2.4 to 2.5 / 5.1 to 5.9 GHz	2.4 to 2.5 / 5.1 to 5.9 GHz
Antenna Type	Omni-directional	Directional, Panel
Typical Antenna Gain	6/9 dBi	15/18 dBi
Impedance	50±5 ohms	50±5 ohms
Polarization Linear	Linear	Linear
HPBW/Horizontal	360°	50/10°
HPBW/Vertical	10/8°	30/10°
V.S.W.R.	1 : 1.5 Max.	1 : 1.5 Max.
Power Handling	10 W Max.	20 W Max.
Connector(s)	N-type (female)	N-type (female)
Operating Temperature	-40 to 80°C	-40 to 80°C
IP Rating	IP65	IP65
Antenna Profile	260 mm length	270 x 205 x 15 mm
Weight	155 g	1020 g

IEEE 802.11a 5 GHz Wireless Antennas

Product Name	ANT-WSB5-ANF-12	ANT-WSB5-PNF-18
Antenna Patterns	E-Plane H-Plane	E-Plane H-Plane
Frequency Range	5.1 to 5.9 GHz	5.1 to 5.9 GHz
Antenna Type	Omni-directional	Directional, Panel
Typical Antenna Gain	12 dBi	18 dBi
Impedance	50±5 ohms	50±5 ohms
Polarization Linear	Linear	Linear
HPBW/Horizontal	360°	10°
HPBW/Vertical	6°	10°
V.S.W.R.	1 : 1.3 Max.	1 : 1.5 Max.
Power Handling	10 W Max.	10 W Max.
Connector(s)	N-type (female)	N-type (female)
Operating Temperature	-40 to 80°C	-40 to 80°C
IP Rating	IP65	IP65
Antenna Profile	420 mm length	270 x 205 x 15 mm
Weight	430 g	990 g

Cellular Antennas

	GSM/GPRS Cellular Antennas				UMTS/HSDPA/WCDMA Cellular Antennas	
Product Name	ANT-CQB-ASM-01	ANT-CQB-AHSM-00-3m	ANT-CQB-AHSM-03-3m	ANT-CQB-AHSM-05-3m	ANT-WCDMA-ASM-1.5	ANT-WCDMA-AHSM-04-2.5m
Frequency Range	850/900/1800/1900 MHz	850/900/1800/1900 MHz	850/900/1800/1900 MHz	850/900/1800/1900 MHz	850/900/1800/1900/2100 MHz	850/900/1800/1900/2100 MHz
Cable Type	---	RG174/U	RG174/U	RG174/U	---	RG174/U
Typical Antenna Gain	max. 1 dBi	0 dBi	3 dBi	5 dBi	1.5 dBi	4 dBi
Impedance	50 ohms	50 ohms	50 ohms	50 ohms	50 ohms	50 ohms
Polarization Type	Linear	Linear	Linear	Linear	Vertical	Vertical
V.S.W.R.	---	< 2	< 2	< 2	1 : 6.4	< 2
Connector(s)	SMA(M)	SMA(M)	SMA(M)	SMA(M)	SMA(M)	SMA(M)
Antenna Profile	3.3 mm length	100 mm length	250 mm length	370 mm length	104 mm length	110 mm length
Cable Length	---	3 m	3 m	3 m	---	2.5 m

Moxa Performance Test Report

ANT-WDB-O-2(Omni dipole dual band 2dBi antenna)

Distance(Km)	0.1	0.2	0.5	1
2.4G-AP → Station (Mbps)	18.38	16.62	7.869	4.471
2.4G-Station → AP (Mbps)	20.13	17.471	6.82	4.008
5G-AP → Station (Mbps)	20.371	11.725	12.959	N/A
5G-Station → AP (Mbps)	19.068	13.637	13.123	N/A

N/A: Not Available

ANT-WSB-ANM-05(Omni dipole 2.4G 5dBi antenna)

Distance(Km)	0.1	0.2	0.5	1
2.4G-AP → Station (Mbps)	24.257	17.597	10.781	4.965
2.4G-Station → AP (Mbps)	20.67	20.315	10.246	5.922

N/A: Not Available

ANT-WSB-ANF-09(Omni directional 2.4G 9dBi antenna)

Distance(Km)	0.1	0.2	0.5	1	2.3
2.4G-AP → Station (Mbps)	18.725	17.557	12.678	7.649	9.259
2.4G-Station → AP (Mbps)	20.452	19.953	15.259	6.637	9.855

N/A: Not Available

ANT-WSB5-ANF-12(Omni directional 5G 12dBi antenna)

Distance(Km)	1	2.3	5.3	10
5G-AP → Station (Mbps)	11.92	N/A	N/A	N/A
5G-Station → AP (Mbps)	9.259	N/A	N/A	N/A

N/A: Not Available

ANT-WSB-PNF-12(Uni-directional 2.4G 12dBi antenna)

Distance(Km)	1	2.3	5.3	10
2.4G-AP → Station (Mbps)	11.92	15.579	8.02	N/A
2.4G-Station → AP (Mbps)	11.905	16.078	8.022	N/A

N/A: Not Available

ANT-WDB-PNF-1518(Uni-directional dual band 15/18 dBi antenna)

Distance(Km)	1	2.3	5.3	10
2.4G-AP → Station (Mbps)	15.686	11.892	11.066	0.306
2.4G-Station → AP (Mbps)	14.703	13.176	11.691	0.204
5G-AP → Station (Mbps)	24.519	12.889	6.934	N/A
5G-Station → AP (Mbps)	25.001	15.035	7.553	N/A

N/A: Not Available

ANT-WSB5-PNF-18(Uni-directional 5G 18dBi antenna)

Distance(Km)	1	2.3	5.3	10
5G-AP → Station (Mbps)	25.022	16.75	9.662	N/A
5G-Station → AP (Mbps)	26.456	18	9.508	N/A

N/A: Not Available

ANT-WSB-PNF-18(Uni-directional 2.4G 18dBi antenna)

Distance(Km)	1	2.3	5.3	10
2.4G-AP → Station (Mbps)	19.627	23.552	14.168	9.715
2.4G-Station → AP (Mbps)	18.051	21.22	15.564	8.559

N/A: Not Available

2.5 Mobile Optimization

In mobile applications that involve multiple access points (APs), the speed and roaming (handover) mechanism can be crucial to a project's success. In the world of wireless, roaming refers to when a client moves between two or more access points. As a result, seamless connection is required for the client to roam from one AP to another.

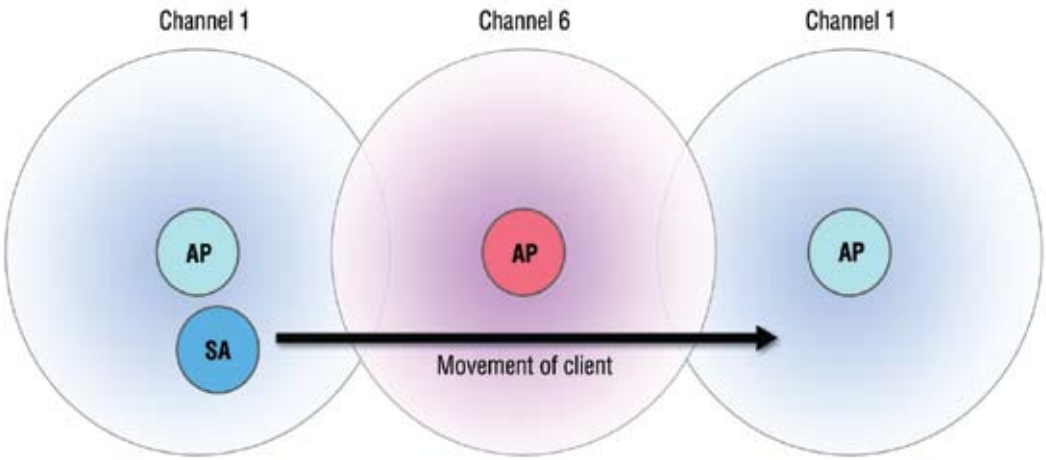
Simply put, as the client physically moves from one AP to another, the signal from the first AP will drop while the signal strength from the other AP will increase. By the time the signals from the first AP drop below the signals from the second AP, the client will have roamed to the second AP.

There are a number of factors that will affect the smoothness of roaming. These include the topology of the access points, gain and coverage of the antennas, and the roaming threshold settings on the client. To ensure smooth roaming, we first have to take into consideration the routes of the moving object and carefully plan the wireless AP deployment configuration.

Different applications encounter different roaming conditions, but we will use linear roaming as an example to illustrate how roaming is conducted and what factors we need to pay special attention to.

Roaming Under Linear Movement

A client is moving from left to right across three different APs. As the client moves, the signal from the first AP drops and the signal strength from the second AP increases. Most of the commercial wireless clients only monitor the communication quality as the basis for roaming decisions. That is to say, when the signal from first AP drops and frames can not be transmitted, the client, in an IEEE 802.11b application, will first drop the communication speed from 11 Mbps to 5.5 Mbps and then to 2 Mbps and 1 Mbps. If the communication quality is still poor and frame transmission continues to fail, the client will decide to roam from the first AP to the second AP.



A roaming mechanism of this sort might be able to satisfy many non-critical applications. However, this type of mechanism severely impairs the smoothness of data transmission for video or audio applications, which require higher quality data transmission.

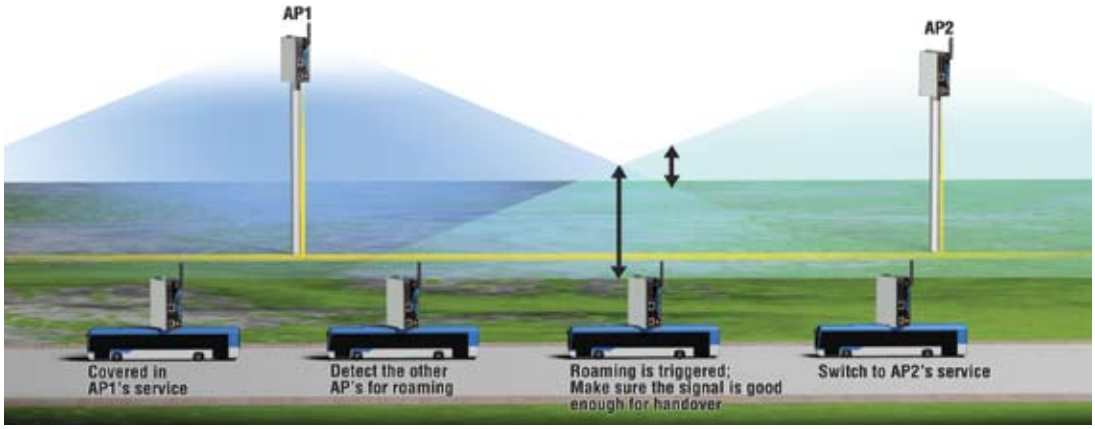
Limitations of High Speed Roaming

The first limitation of the Threshold-based Handover Algorithm is wireless resource consumption because the client is constantly scanning for APs that also need to respond in due time. To solve this problem, the network topology and system configuration needs to be carried out in greater detail.

The second limitation is that there is currently no unified high speed roaming standard so roaming among different APs from different manufacturers might not be possible.

Roaming Speed Acceleration

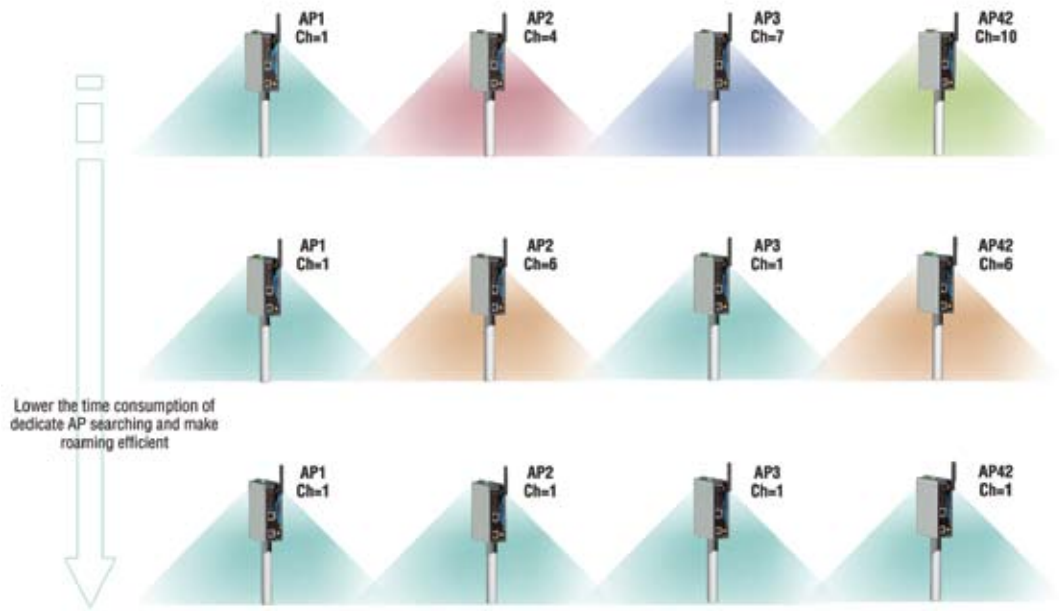
To increase the roaming speed, a common method is to use the Threshold-based Handover Algorithm.


AP1
AP2
Covered in AP1's service
Detect the other AP's for roaming
Roaming is triggered; Make sure the signal is good enough for handover
Switch to AP2's service

The Threshold-based Handover Algorithm allows roaming only when the current AP's signal drops below a certain threshold so that roaming to another AP would improve the transmission quality and at the same time provide a stronger signal.

In short, the Threshold-based Handover Algorithm means the client will constantly scan for the best AP signal quality and roam only when the threshold is reached. This can prevent the ping-pong effect, unnecessary handovers that might take place when the client moves back and forth between two APs. Also, this can increase the roaming speed to deliver a smoother data transmission.

The second way to increase the roaming speed is to unify AP channels to avoid wasting channel hopping time during roaming. However, a unified channel selection will also cause interference. Users are advised to make proper channel separation among roaming APs to reduce interference.

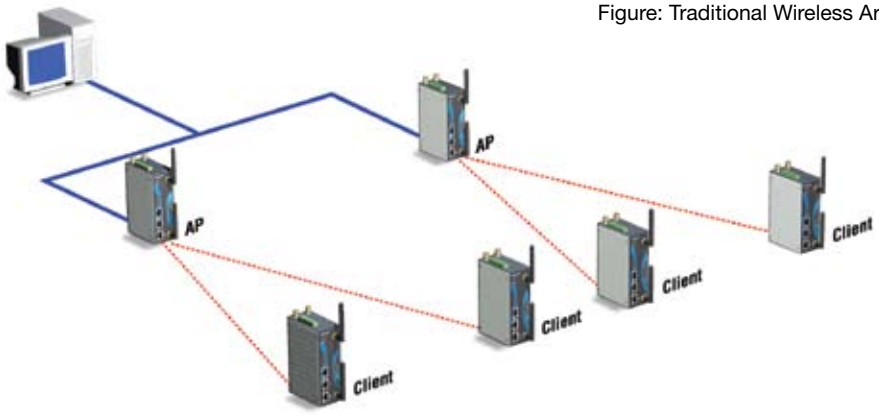


2.6 Advanced WLAN Technologies

Dual RF Redundancy

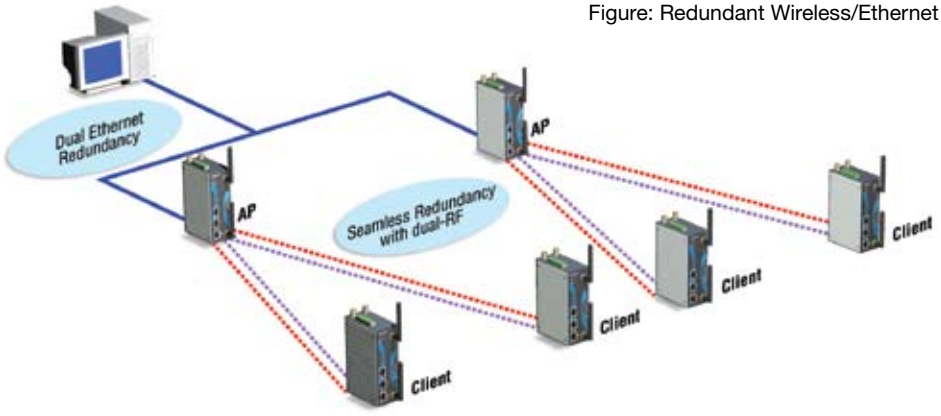
According a recent VDC report, more than 40% of wireless users are concerned about interference. In industrial and critical applications, this issue is even more important. Normally, interference occurs in a dedicated frequency. So, if we can use 2 or more different frequencies to communicate at the same time, then data transmission will not be stopped, even if there is interference in one of the frequencies. The picture below depicts the standard architecture for wireless infrastructure. As you can see, access points (AP) can connect many Clients to an Ethernet network.

Figure: Traditional Wireless Architecture



For network redundancy, simply use APs and Clients with dual RF and keep the existing architecture (usually, these 2 RFs are set to 2.4 GHz and 5 GHz to make sure prevent interference). To ensure that data can be delivered between the AP and Client, even when there is interference in one of the frequencies, Moxa devices are equipped with a special protocol with almost '0' switching time for seamless redundancy. For reliability beyond wireless redundancy, Ethernet redundancy is also required. Fast ring redundancy like RSTP or Turbo Ring is important on the Ethernet side.

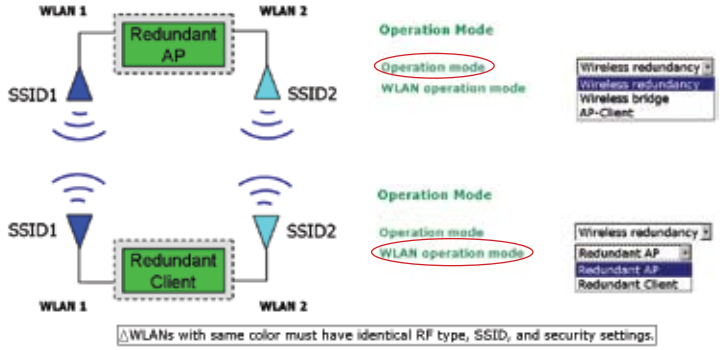
Figure: Redundant Wireless/Ethernet Typology



Introduction to Moxa's Dual RF Redundancy

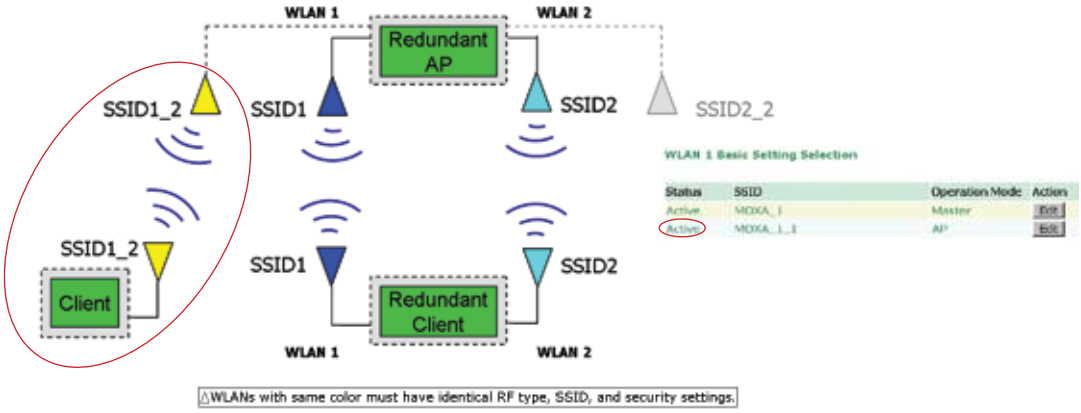
Moxa's advanced AP/Client AWK-5000/6000 series product line provides this kind of redundancy. The configuration is very easy. All you need to do is select redundant AP on the AP side and redundant Client on the client side. Then, set a different SSID for each RF. As shown in the following figure depicting the Web console UI for Moxa's AWK-5222, set SSID1 for WLAN1 and SSID2 for WLAN2.

Figure: Dual RF—Wireless Redundancy Mode



If both the existing Clients and dual RF clients support redundancy in the same network, Moxa's AWK-5000/6000 Access Point can connect both types of clients to an Ethernet network. As shown in the figure below, enter SSID (Moxa_1_1) in the 2nd column for the AP to connect the traditional wireless clients with this SSID to the AP.

Figure: Single RF Connection

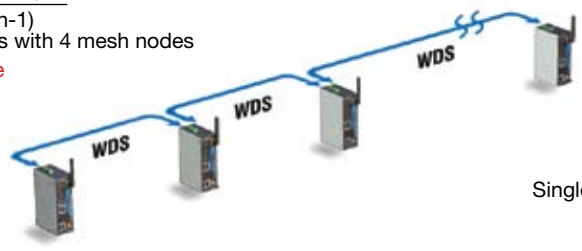


In addition to wireless redundancy mode, Moxa's AWK-5000/6000 advanced AP/Client devices offer another dual RF feature called "Wireless Bridge" mode. This is designed to optimize WDS mode because of the throughput problem for WDS. The normal eruption for throughput is throughput = 25Mbps/(n-1), where n is the nodes number for WDS. With Wireless Bridge mode, we can keep the throughput at 10 to 15 Mbps. Configuration is simple; simply link the Wireless Bridge master to the Wireless Bridge slave, as shown below.

$$\text{Throughput} = \frac{25\ \text{Mbps}}{(n-1)}$$

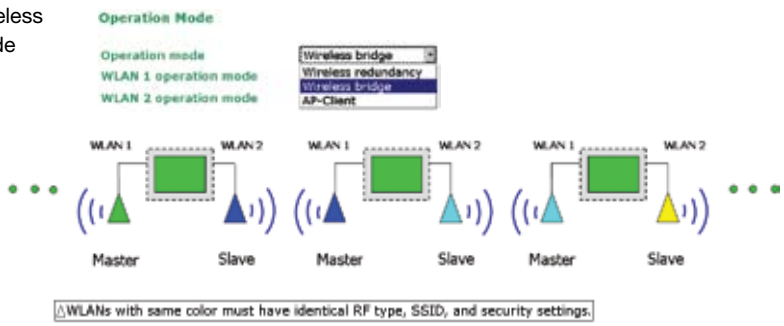
Ex. Around 8Mbps with 4 mesh nodes

Poor Performance



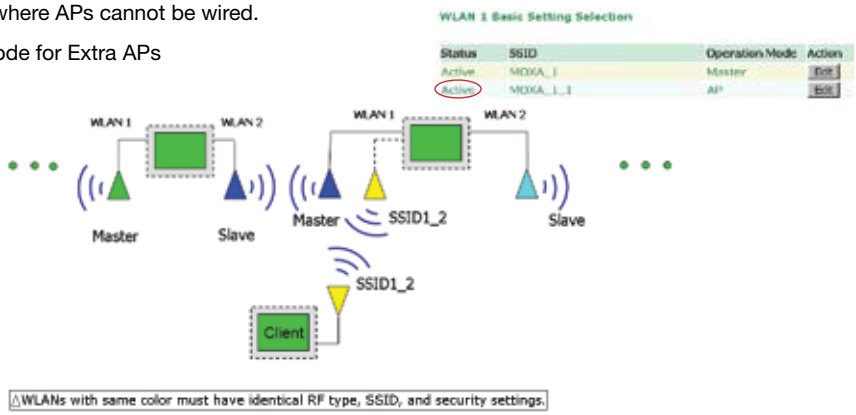
Single RF—Mesh Network

Figure: Wireless Bridge Mode



Wireless Bridge mode can also connect wireless clients to another SSID, as shown below, so it can be used in environments where APs cannot be wired.

Figure: Bridge Mode for Extra APs



Mesh Technologies

Mesh technologies are generally considered to be wireless communication systems that are interconnected to each other. However, there are two distinctive ways to build up a so called mesh network: wireless distribution systems (WDS) and mesh routing. Both of these methods create Layer 2 connections to one or more bridges / mesh routers to allow data to be passed between them.

WDS differs from mesh routing in many ways. Generally WDS has the nature of a more static network configuration without significant demand for redundancy. That is, a wireless bridge is configured to point to the adjacent bridge with a predefined MAC address. So when a bridge fails and while there is no adjacent bridge is configure to serve as a backup path, the link will be lost.

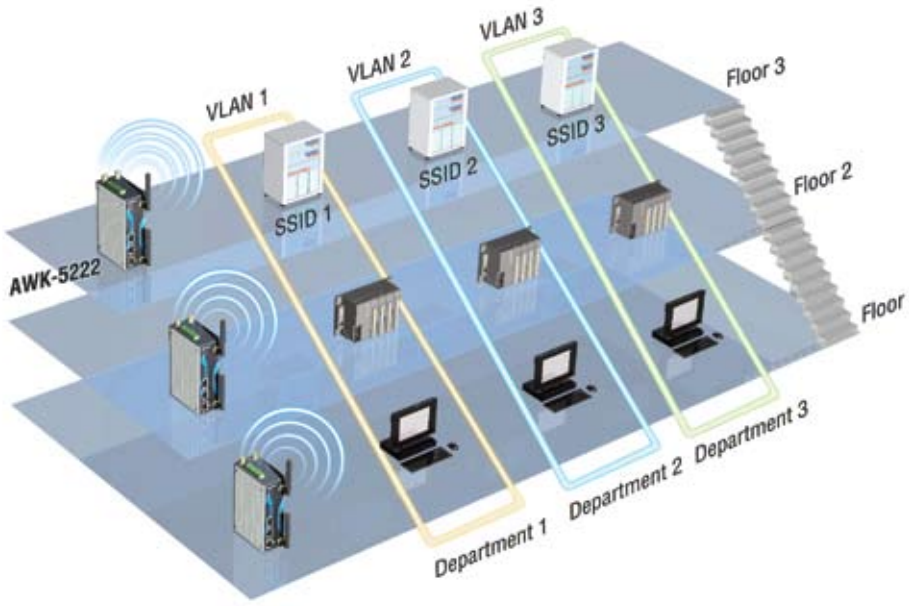
A wireless mesh routing link, on the other hand, can provide greater redundancy because it can create a redundant path in the event of node failure. In other words, the mesh router automatically detects a new node when the original node fails and dynamically determines the best path.

While a WDS is more of a standard and a mesh routing link is more of a proprietary standard, they are being adopted in accordance with users' needs. A WDS is often employed in a hierarchical network topology for bridges that can not prevent broadcast storms. As a result, a WDS is often configured in spanning tree topologies. A bridge loop is often avoided to prevent a broadcast storm. However, there are software solutions which utilize Spanning Tree Algorithms (STA) to compute the best path between two nodes while putting all other paths in blocking mode. This realizes communication redundancy in a WDS but it can be time consuming to create a workable bridge loop. So a WDS is often adopted in a small network that requires manual configuration for each node. Once the connection is established, it is not easily interrupted.

Mesh routing on the other hand is often adopted in systems that require higher redundancy. It often needs few manual configurations for each node and provides greater expandability when more nodes are to be added in the future. In summary, redundancy is the primary concern when choosing mesh routing links. It is also more of a suitable choice when the connections are subjected to constant disruptions, for example, by passing by buses.

Wireless VLAN

A Virtual LAN (VLAN), as defined in IEEE, is a group of hosts grouped together as if they were attached to the Broadcast domains in a Layer 2 network. Traditional networks use routers to define broadcast domain, but it is now possible to set the broadcast domain boundaries with Layer 2 switches. That is to say, a VLAN can add two or more hosts that were in different subnets to be grouped into the same LAN segment disregard of their geographical locations. VLAN provides the leeway to the network administrators to address network security, management and scalability issues.



How to Set Up VLAN with IEEE 802.11

Every time a packet is sent from one switch to another over a VLAN, VLAN tagging is required. VLAN tagging is the practice of inserting a VLAN ID in the packet header so the packet can be identified and forwarded to the right port or interface. The IEEE 802.1q standard is the most commonly seen VLAN tagging protocol created by IEEE group. The tagging protocol supports a maximum of 4096 VLANs.

By borrowing the same concepts, it is now also possible to apply VLAN to an IEEE802.11 wireless network. Many wireless access points (AP) are now equipped with VLAN capability. A single AP can now be configured to assign a different service set identifier (SSID) to different VLANs. Also the authentication settings like MAC, EAP, and VLAN ID are required to configure a wireless VLAN.

Wireless VLAN Limitations

Wireless VLANs bring many benefits to WLAN applications, but there are some potential limitations when a wireless VLAN reaches a certain scale. The first limitation arises from its 12 bit VLAN identifier (VID). The size of the VID limits the number of wireless VLAN to 4094. The number might look big enough to accommodate most WLAN applications. However, as wireless applications grow at a tremendous pace, it will soon be not enough for some large scale WLAN applications.

Large scale Wireless VLAN also causes the second and third limitations. That is, when the Wireless VLAN grows too large, traffic flowing through the routers also increases. This large volume of traffic makes routers another potential bottleneck for the Wireless VLAN.

The third constraint is the potential security loopholes. As the VLAN grows, there is a possibility that the wireless VLAN will stretch over large geographical areas that require the VLAN to pass through a third party network. This creates security loopholes as there is almost nothing to stop the virus from spreading inside the VLAN.

QoS for Video/Audio and Control

The dramatic growth of WLAN has also led to demands for video and audio transmission over WLAN. Quality of Service (QoS) is therefore becoming an important topic for wireless communications. QoS is a network term for controlling and measuring data transmission rates, throughputs and error rates. QoS is not of a big concern for simple data transmission. However, it becomes more of an issue when it comes to audio and especially video. Video requires high quality of flow and throughput control and lower error rates. All these are In multimedia data transmission, it is important for delays arising from network latencies to be undetectable to users.

IEEE 802.11e was set up to answer this call for QoS in WLAN. IEEE 802.11e is the amendment that defines wireless LAN QoS enhancement in IEEE 802.11. WLAN QoS is achieved through modifications to the Media Access Control (MAC) layer, solving the latency delay problem that is sensitive to multimedia and voice data transmission.

Wireless Management

QoS is essential for wireless communication. It is an important element for wireless applications when it comes to management. There are three layers of management, namely device management, network management, and centralized management.

Device Management

When it comes to network management, device management is always the most basic task for all network administrators. Often, wireless APs/Clients come with a management utility or web console that allows network managers to locate and remotely configure the wireless APs/Clients.

Network Management

Above device management is the network management layer. This layer requires a higher level of software utilities to manage all wireless nodes. The network management utility should be able to perform multiplatform monitoring, event management, alerting, real-time performance monitoring, network discovery, and topology mapping.

Centralized Management

More advanced network management tools provide a complete solution for network administrators including VPN, firewall, and UTM. It also allows centralized management for device maintenance.

2.7 Industrial Certification

EN50155 Certification

EN50155 are the standards that define requirements for railway cars, or rolling stock. It clearly outlines the requirements for power input voltage fluctuation, transient, ambient temperature ranges, shock and vibration and as well as fog and salt spray. Electronics that are used aboard railway rolling stock are required to meet the standards of EN50155. The target of EN50155 certification for all electronics is for the devices to be operable 24/7 for as long as 20 years. To meet this standard, an electronic device needs to meet the requirements as summarized below:

Power Input Voltage Fluctuation

A nominal 110 VDC power input system needs have at least 77 to 137.5 VDC voltage fluctuation range with no time limits. The fluctuation may sometimes become too extreme so electronic devices should also be able to withstand 66 to 154 VDC power input for at least 100 ms.

Transient and Ambient Temperature

Railway rolling stock require an operating temperature range of -25 to 40°C, or -40 to 85°C, for electronic devices. When the trains enter and leave a tunnel, the temperature change can be very drastic. As a result, electronic devices must also be able to withstand a 3°C/sec temperature change and thermal shock that leads to condensation on the PCB.

Shock and Vibration

EN50255 follows the test standards of EN67373. Electronic devices must withstand at least 1 G vibration when mounted on a DIN-Rail. Chassis mounted devices are required to withstand a shock rating as high as 50 G.

Atmospheric Pollutants

Combustible dust accompanied by oil, sulphur dioxide, and salt spray in the air create a hazardous environment for rolling stock applications. As a result, an EN50155 compliant device must have a high IP rating.

Air Cooling

Force air cooling systems are not allowed. EN50155 electronic devices must have conductive-only mechanism designs to eliminate potential maintenance problems that arise from fan cooling systems.

Moxa AWK Series Meet EN50155 and EN50121-3-2/50121-4 Standards for Rail Traffic

Certified to Meet Industry Standards Rail vehicles require the highest standards of stability due to random vibrations that occur during normal operation. The EN 50155 standard covers electronic equipment used on rolling stock, and EN 50121-4 defines the emission and immunity of signaling and telecommunication apparatus. They outline the issues that need to be addressed to ensure that railway electrical systems are integrated successfully.

The AWK series is engineered to resist extreme vibrations and shocks based on the railway standards (EN50155/EN50121-3-2/50121-4).

Rail Traffic

- EN 50155 (Environmental)
- EN 50121-3-2 (EMC)
- EN 50121-4 (EMC)

ATEX/Class I Division 2

ATEX is the term used when referring to the European Unions (EU) Directive 94/9/EC. ATEX governs the regulations on the equipment used in potentially explosive atmospheres. All equipment meeting the requirements are free to circulate within EU boarders. The directive applies to all equipment or protective systems used in areas subject to explosion risks, gas vapors, mist, or dust. The directive also sets the standards for safety devices, control equipment, and calibration equipment.

About ATEX/Class I Division 2

Class I Division 2/Zone 2

Class I Locations:

These locations are defined as places where the air may contain flammable gases or vapors in sufficient quantities to cause explosive or ignitable mixtures.

Division 2:

The division defines the conditions under which the hazard exists. Division 2 refers to the following conditions:

- Liquids and gases in closed containers or systems are handled, processed, or used.
- Concentrations are normally prevented by positive mechanical ventilation.
- The specified area is adjacent to a Class I, Division 1 location.

Zone 2:

This is defined as an environment where an explosive gas atmosphere is not likely to occur during normal operation, but could occasionally arise for brief periods of time.

ATEX/Class I Division 2 in Oil & Gas Industry

Safety is of the utmost importance and cannot be negotiated in dangerous industrial environments. In particular, oil and gas exploration sites, as well as energy field development, production, and transportation facilities face a real risk of explosions. Therefore, engineers must ensure prior to installation that all the equipment and protection systems have to meet or exceed regulatory standards used under hazardous conditions.

Moxa Offers Specifically Designed for Hazardous Sites

Designed with the highest safety standards in mind, Moxa's AWK series of WLAN solutions are constructed in strict accordance with global acceptance for explosion protection in hazardous locations. Product offerings include rugged AWK-3121 and AWK-4121. With ATEX/Class 1 Division 2, and UL C1D2 certifications, these stringently proven WLAN products help build safe and reliable networks in the oil and gas industry.

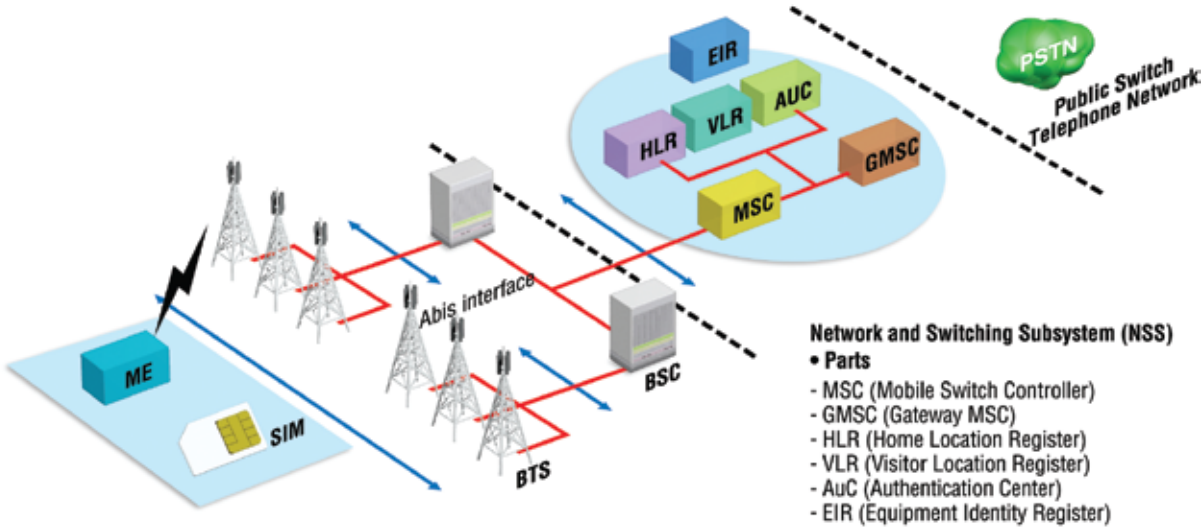
Chapter 3
Cellular Networks

3.1 Cellular Basics

What is Cellular?

Cellular is a radio based communications system that enables customers to call and be reached over a wide area, supporting both hand-over and roaming. Cellular networks are connected to the PSTN to give transparent incoming and outgoing access to fixed network subscribers.

The following diagram shows a typical GSM cellular network architecture:



Network and Switching Subsystem (NSS)
- **Parts**
- MSC (Mobile Switch Controller)
- GMSC (Gateway MSC)
- HLR (Home Location Register)
- VLR (Visitor Location Register)
- AuC (Authentication Center)
- EIR (Equipment Identity Register)

Base Station Subsystem (BSS)
- **Parts**
- Base Transceiver Station (BTS)
- Base Station Controller (BSC)

Mobile Station (MS)
- **Parts**
- Mobile Equipment (ME)
- Subscriber Identity Module (SIM)

Supports the switching functions, subscriber profiles, and mobility management

- Radio Interface Connects to MS
- A Interface Connects to MSC

Moxa OnCell G2100/3100 series, PDA or PC connected to the ME

Data Service of GSM

Here we show how to implement these three data services. We hope this will help you understand how these technologies work so you can select the most suitable application.

Short Message Services (SMS)

SMS messages, as specified by the ETSI organization (documents GSM 03.40 and GSM 03.38) and can be up to 160 characters long, where each character is 7 bits according to the 7-bit default alphabet. Eight-bit messages (max. 140 characters) are usually not viewable on phones as text messages. Instead, they are used for data in 16-bit messages (max. 70 characters) and used for Unicode (UCS2) text messages viewable on most phones.

SMS is a point-to-point store and forward technology with 2 basic functions:

- Transmit a message from the short message service center to the mobile station. SMS-DELIVER PDU (Protocol Data Unit)
- Transmit a message from the mobile station to the service center. SMS-SUBMIT PDU (Protocol Data Unit)

SMS messages contain up to 140 octets which is equivalent to

- 160 Latin characters (7 Bit Coding) in Text Mode, or
- 70 Unicode characters (double byte), such as Arabic or Chinese characters.

SMS Summary

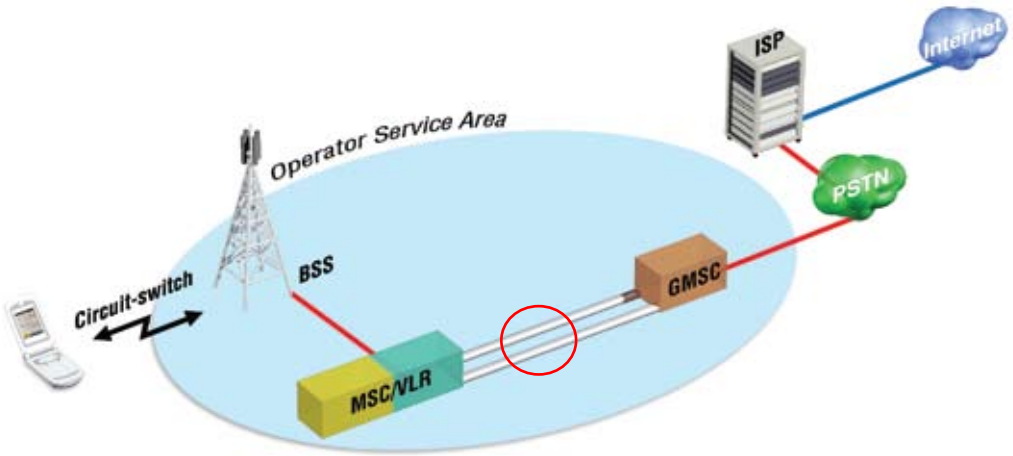
- Up to 140 octets or 160 characters for every message
- No IP-based communication, only suitable for sending/receiving serial data

Circuit Switch Data (CSD)

Circuit Switched Data (CSD) is the original form of data transmission developed for Time Division Multiple Access (TDMA) based mobile phone systems like Global System for Mobile Communications (GSM). GSM CSD bearer service is the most widely used data service providing a “non-transparent” data rate of 9.6 Kbps. “Non-transparent” in this context means error correction and flow control.

Usually, GSM network operators support the non-transparent CSD bearer service through a modem interworking function. This means that a mobile station (mobile phone) initiates a data call and the network routes the call to the modem interworking function, which is located at the Mobile Switching Center (MSC) of the GSM network, which then dials the number supplied by the mobile station.

Confirm that your cell phone service provider allows fax/data type connections for your cellular service plan. Please note that we are not referring to high-speed wireless data services or SMS. We are referring to your cellular service plan’s ability to transmit a “fax call” connection, which has been widely included in cellular service plans for years. This feature is typically referred to as CSD (circuit switched data).



- **CSD Summary**
  - Up to 9.6 Kbps
  - Circuit-switched connection
  - IP-based communication possible with dedicated link, but speed is slow and billed by connection setup, most operators remove CSD service
  - Most GSM operators provide the service
  - In North America, CSD has been completely phased out by the end of 2007

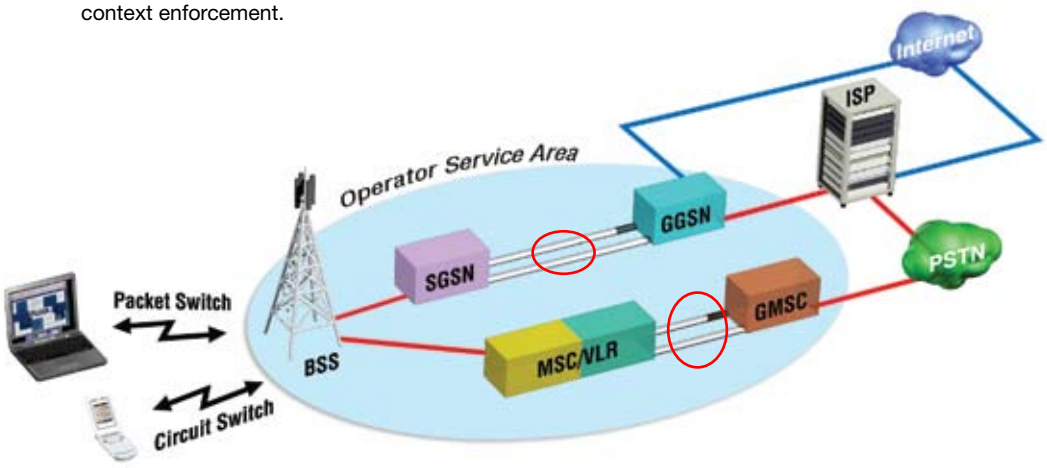
Packet Switching Data Solution: GPRS

General Packet Radio Service (GPRS) provides Packet Switching service to GSM systems. A GSM system is traditionally a Circuit Switching network that provides optimized voice transmission service. For instance, a call between Party A and Party B will exclude other parties. Even if Party A and Party B temporarily fall into silence during their conversation, the call (network resource) won't be released until either end hangs up. As a result, the network resource is wasted when a data call is utilized in a GSM network. That is because data transmission doesn't necessarily need real-time transmission, which is primarily required for voice or video communications. A few seconds delay won't change the correctness and consequence in data transmission. Take email uploads and downloads for example. The network resource is occupied only when data is transmitted through the packet switching system. As a result, other users can freely send their data when the system is "inactive." Accordingly, consumers benefit from the low cost and real-time data transmission of GSM networks.

General packet radio service (GPRS) is a packet-oriented mobile data service available to 2G and 3G GSM users.

A GSN (GPRS Support Node) is a network node that supports the use of GPRS in the GSM core network. All GSNs should have a Gn interface and support the GPRS tunneling protocol. There are two key variants of the GSN, namely Gateway (GGSN) and Serving GPRS Support Node (SGSN).

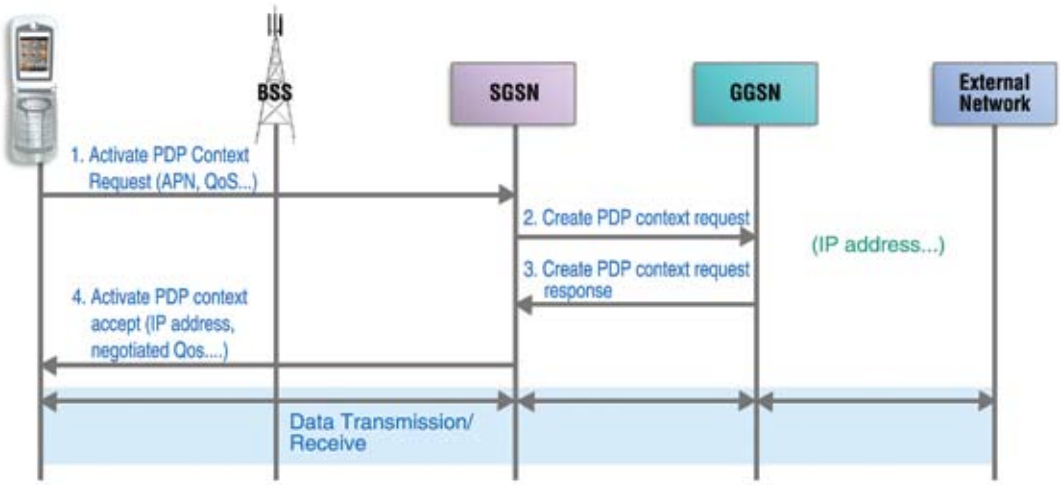
- **Serving GPRS Support Node (SGSN)**
  A Serving GPRS Support Node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles (e.g., IMSI (ID code of the SIM card) addresses used in the packet data network) of all GPRS users registered with a particular SGSN.
- **Gateway GPRS Support Node (GGSN)**
  The Gateway GPRS Support Node (GGSN) is a main component of GPRS networks. The GGSN is responsible for connecting the GPRS network to external packet switched networks such as the Internet and X.25 networks.
  The GGSN stores the current SGSN address of the user and his or her profile in its location register. The GGSN is responsible for IP address assignment and is the default router for the connected user equipment (UE). The GGSN also performs authentication and charging functions.
  Other functions include subscriber screening, IP Pool management and address mapping, QoS and PDP context enforcement.



- **Summary**
  - General Packet Radio Service (GPRS)
  - Connectionless
  - Bill by packets
  - IP-based communication, Internet access and increasing speed with 3G, HSDPA, HSUPA, etc.

APN in Packet Switch

Each external network is given a unique Access Point Name (APN) that is used by the mobile user to establish the connection to the required destination network.



PDP context activation procedures are as follows:

1. Mobile phone sends out PDP context activation request and other relative parameters (e.g.,APN, QoS)
2. SGSN begins verification based on previously stored GPRS Attach information
3. DNS mechanism in SGSN analyzes the APN and returns a GGSN address
4. SGSN and GGSN build logic links
5. GGSN will instruct an IP address for the mobile phone and send it to the MS via SGSN. The external network can then start a session with the MS.

- **APN (Access Point Name)**
  - Access Point Name is a label according to DNS naming conventions describing the access point to the external packet data network (PDN).
  - An APN is a logical way to name a GPRS service.
  - The Domain Name Service (DNS) server translates the APN into the GGSN IP address.
  - APN string naming comes from the mobile operator. There is no common rule so customers need to request (1) GPRS service and (2) the APN string from their operator.
  - Some operators offer different APNs according to the GPRS service level, such as public fixed IP addresses, non-port blocking, or VPN.

- **IP Address Allocation in GPRS**
  - Fixed addressing
    IP address is stored in HLR
    HLR sends IP address to SGSN, then SGSN sends IP address to the MS
    IP address is sent to the MS when the MS wants to send data
  - Dynamic addressing
    GGSN receives the IP address (DHCP/local address pool/RADIUS)
    When the MS opens PDP context, GGSN assigns an address to the MS

- **Obtaining an IP Address**
  - From a local address pool on the GGSN
  - Via DHCP
  - Via RADIUS from an external RADIUS server
  - From the customer's network via an L2TP tunnel from the GGSN

3.2 Private IP Solution

There are two limiting factors you are almost assured to encounter when setting up a wired LAN with private IP addresses in an office: (1) short transmit latency and (2) limited IP addresses to connect to the Internet for the cellular WAN interface. As a result, delay times for the WAN interface are very different from the local area network's delay times. WAN port IP addresses are also very different from those in office LANs.

Private IP vs. Public IP

From the LAN point of view:

According to RFC 1918 standards, office networks are allocated private IP addresses according to class A, B, and C. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP address space for private networks:

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

From the cellular WAN port point of view:

Normally, IP addresses for cellular WAN ports will have:

Type of Address	Description	Role(s) of Configured Devices
Floating private IP address	Mobile operator keeps a pool of private IP addresses and assigns one to the GPRS subscriber	Always Client role to access server Class A 10.xx.xx.xx
Floating public IP address	Mobile operator keeps a pool of public IP addresses and assigns one to the GPRS subscriber	Can be Client or Server role, IP address is always changeable, needs a notification mechanism to update public IP address
Fixed public IP address	Mobile operator keeps a dedicated IP address for each SIM card based on the SIM card's (IMSI) ID code and user service level	Can be Client or Server role, IP address is fixed, needs a special bill rate from operator

As you can see from the table above, the kind of WAN IP address obtained from your cellular operator will affect network planning and determine the role of the devices configured with the IP address.

Private IP addresses are suitable for Client role.
Public IP addresses are suitable for Client role and Server role.

Delay Time

Latency in a packet-switched network is measured either one-way (the time from the source sending a packet to the destination receiving it) or round-trip (the one-way latency from source to destination plus the one-way latency from the destination back to the source). Round-trip latency is more often quoted, because it can be measured from a single point. Note that round trip latency excludes the amount of time that a destination system spends processing the packet. Many software platforms provide a service called ping that can be used to measure round-trip latency. Ping performs no packet processing; it merely sends a response back when it receives a packet (i.e., performs a no-op) so it is a relatively accurate way of measuring latency.

Where precision is important, one-way latency for a link can be more strictly defined as the time from the start of packet transmission to the start of packet reception. The time from the start of packet reception to the end of packet reception is measured separately and called "Serialization Delay." This definition of latency is independent of the link's throughput and the size of the packet, and is the absolute minimum delay possible with the link latency of the LAN you can measure by specified device with input to output delay time in serialization.

As a result of WAN latency from cellular networks, you cannot count the number of nodes in your link as the timing is different for each link. Therefore, delay time in cellular networking is immeasurable and not suitable for real-time systems.

Solution for Private IP

A common problem in M2M network planning is that cellular operators and service providers usually only provide private and dynamic IP addresses. The reasons for doing so are threefold:

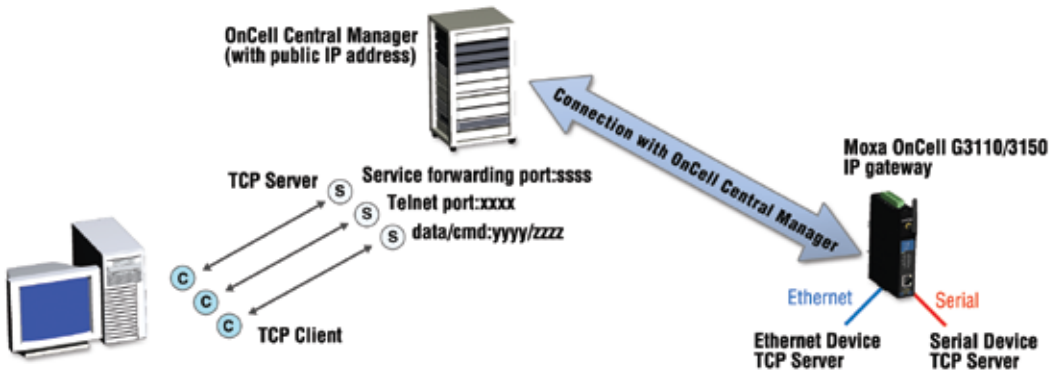
1. In the world of Internet communication, one of the biggest problems is that the number of public IP addresses is running out quickly. It is therefore reasonable that cellular network operators issue private and dynamic IP addresses to conserve valuable public IP resources.
2. The bandwidth of a cellular network is so narrow that it is very vulnerable to cyber attack. Private IP effectively prevents cyber attacks from paralyzing the networks.
3. Require only uplink from cellular device to WLAN. However, in most M2M applications, it is a requirement that data exchange is a two-way communication either from server to client or client to server.

To solve this private IP issue for M2M applications, three major solutions are available:

1. Users can pay extra money to get a public and fixed IP SIM card. This way, cellular M2M system configuration will be very similar to LAN architecture.
2. Users can get cellular VPN services from their ISP (Internet Service Provider) or a second tier operator known as an MVNO (Mobile Virtual Network Operator). They offer services to allow cellular links between nodes in a VPN that uses open connections or virtual circuits in a larger network, such as the Internet. With the help of VPNs, cellular devices act as a VPN client that can initiate a connection with a VPN server building a two-way communication environment for M2M applications.
3. Despite VPN being the most commonly seen solution to the private IP problem in M2M applications, the data exchange inside a VPN can take up too much of the network resources for it requires heavy duty encryption and decryption of data. To save valuable cellular network resources, some M2M solution providers offer a software solution to help customers cope with the private IP problem. That is, manufacturers provide middleware that works as a communication gateway.

Moxa OnCell Central Manager

The OnCell G3100 series is Moxa's cellular IP gateway that connects serial or Ethernet devices to cellular networks. As a leading industrial networking solution provider, Moxa is aware of the private IP issue troubling many of our M2M customers. To solve this problem, Moxa has introduced OnCell Central Manager. Simply install OnCell Central Manager onto a Server PC with a public IP address and register the IP addresses of OnCell devices in your private network on the Client OnCell IP gateway. As soon as the OnCell IP gateway is powered on, it will initiate the connection to OnCell Central Manager. Thanks to OnCell Central Manager, your access points can now communicate with field devices via cellular networks so you don't need to worry about paying extra VPN service fees or wasting valuable cellular network resources.



3.3 Security

One of the major concerns faced by system integrators when adopting an Ethernet solution is the security and confidentiality of data transmissions over the network. Wireless networks are especially vulnerable because they need to transmit data through open air and are vulnerable to sniffing. To protect the security of wireless connections, one of the most commonly seen solutions is the VPN.

The Virtual Private Network (VPN)

A VPN is a computer network that links up two or more networks or nodes by using open connections or virtual circuits. Many people believe that a VPN offers sufficient data transmission security. However, a VPN, by itself, does not guarantee information security. In response to the lack of security when tunneling through the network, L2TP and IPSec are often used to enhance network security.

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used in a VPN. L2TP is sent in a UDP datagram. It contains no security feature on its own so it is often implemented along with IPSec.

IPSec is an open communication standard created to ensure data transmission security over public networks. IPSec is also a Layer 4 security protocol, which is the most widely used way to ensure security for it is a more balanced solution than Layer 1 and Layer 7 security control.

IPSec uses either Authentication Header (AH) or Encapsulating Security Payload (ESP). AH can protect packet headers and data integrity but provides no encryption functionality. On the other hand, ESP provides encryption and conserves the integrity of the packet, but cannot protect the outermost IP header as AH can. ESP is the most commonly used protocol in a VPN because encryption is more of an important requirement in a VPN while header protection is not.

IPSec also contains the Internet Key Exchange protocol that is used to negotiate IPSec Connection Settings, authentication endpoints, and secret keys, as well as to define the security parameters, manage updates, and more.

As far as the data compression technologies go, IPSec uses IP Payload Compression Protocol (IPComp) to compress data before encryption; this also allows communication to be carried out in a more efficient way.

Firewall

Except for data encryption, using a firewall is the most common method to protect both wired and wireless connections from outside attacks. There are multiple ways in which the firewall acts to deny cyber attacks including inspecting data packets for suspicious contents or filtering IP addresses.

The most protection a firewall can offer is to set up a list of accessible IP addresses that limits access from WANs. In most M2M applications, this is the most effective and direct way to protect a LAN from WAN attacks.

Moxa's OnCell IP router offers two kinds of firewall protection for users to choose from. One way is to filter WAN IP addresses to accept or deny WAN connectivity requests. Another way is to set up a virtual server that allows remote users to access the Host or FTP services via a public IP address, and automatically redirects them to local servers in the LAN. This firewall feature will filter out any unrecognized packet to protect your LAN.

3.4 How to Connect Serial Devices to Cellular Networks

Traditional Modems

Serial port connections are very popular in traditional industrial applications but their transmission distance is limited. The Hayes command modem (AT command) offers a good solution for enlarging the transmission distance. It connects two serial devices through PSTN via an AT modem. This traditional modem always occupies the line as a voice call so even when you are not talking (transmitting data), you will still be charged by the minute for staying on the line.

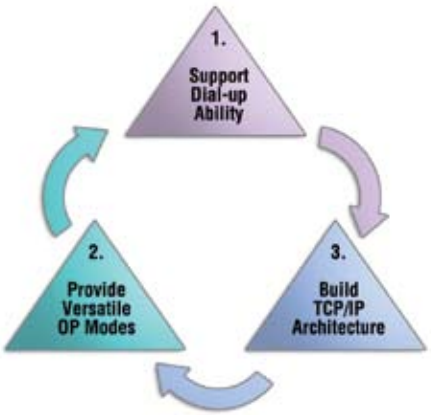
In addition, the serial device (such as a PLC) link to the modem needs dial-up capability for call controls, such as dialing a number, checking if the called side is busy, retrying the call, and hanging up. If the connected link is an IP domain, then the serial device needs built-in PPP (Point to Point Protocol) capability to access the IP domain, whether it is an Internet or VPN. Serial devices also require many call control capabilities in order to link to traditional modems, resulting in heavy loading.

IP modems, equipped with call setup and PPP capability to reach IP Internet domains, offer a viable solution that reduces loading for serial devices so they can focus on transmitting and receiving serial data. Cellular networks are everywhere so you can make calls without a wired telephone connection, providing industrial automation machine-to-machine applications with additional benefits.

IP Gateways

IP gateways are not only call setup intelligent but also come with built-in TCP/IP capability. Due to the popularity of cellular networks around the world, you will be able to use them to communicate from just about anywhere. Moreover, IP gateways can help your serial devices transfer and receive data conveniently.

Moxa's cellular IP gateways solution offers flexible communication for serial devices.



How OnCell Cellular IP gateways can help your serial device access an IP domain:

- Keep existing software (Real COM / Reverse Real COM)
- Standard TCP IP connection (TCP server / Client)
- Real-time serial data send/receive solution
- Short message connection (SMS Tunnel)

Network capabilities for data bearer:

- IP gateways over CSD
- IP gateways over GPRS

Keep Existing Software (Real COM / Reverse Real COM)

Moxa's Real COM and Reverse Real COM operation modes are used to link remote serial devices to the control center. By simply installing OnCell Driver Manager onto a host computer at the control center, your applications will be able to keep existing serial interface software to transfer and receive data from the serial devices.

Here's how it works:

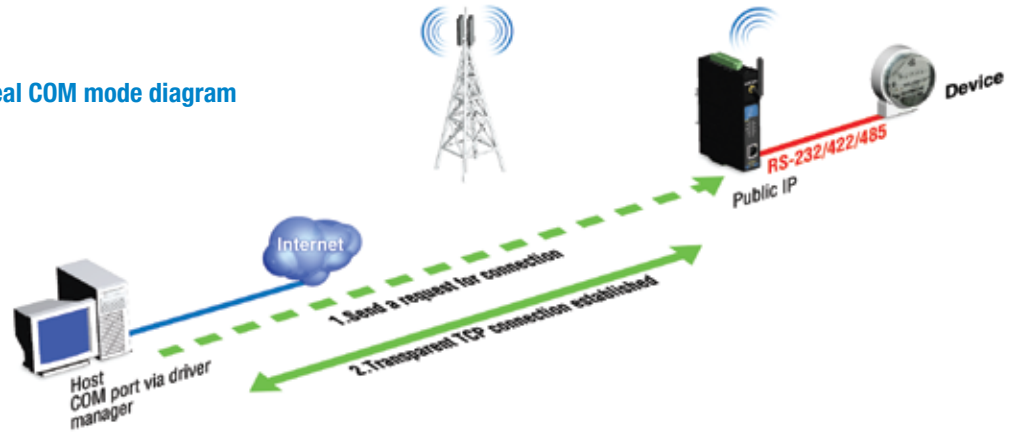
- Installing OnCell Driver Manager onto the host PC allows the host PC to connect directly to remote serial device.
- The serial device is connected to the OnCell G3100's serial port.
- The connection is maintained automatically between OnCell Driver Manager and the OnCell G3100 device to access the serial device over a cellular network.

- Depending on whether the OnCell G3100 device is acting in a Client role or Server role, the user can select Real COM mode or Reverse Real COM mode. Normally, the role of the OnCell G3100 device depends on the IP address obtained from your cellular service provider. If your OnCell G3100 device's SIM card is able to obtain a public IP address, then the OnCell device can act as a Server and you can select Real COM mode to connect the host PC (Client role).

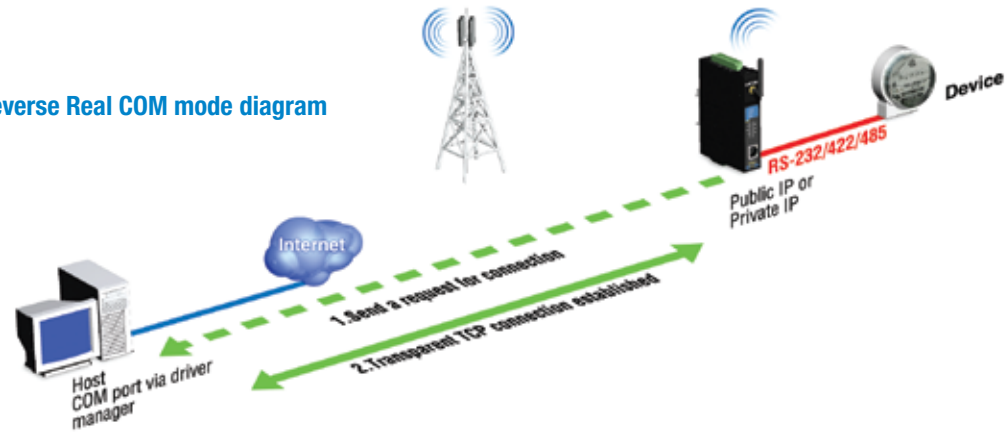
OnCell Device's IP Address	Suitable Role	Operation Mode Selection
Public address	Server role,	Real COM mode,
	Client role	Reverse Real COM mode
Private IP address Like 10.x.y.x or 172.xx.....	Client role	Reverse Real COM mode

If both the host PC (at the control center) and the OnCell G3100 device have private IP addresses, you can use Real COM mode on the OnCell G3100 to resolve the private IP to private IP problem.

Real COM mode diagram



Reverse Real COM mode diagram



Socket Mode, Standard TCP IP Connection (TCP Server/Client)

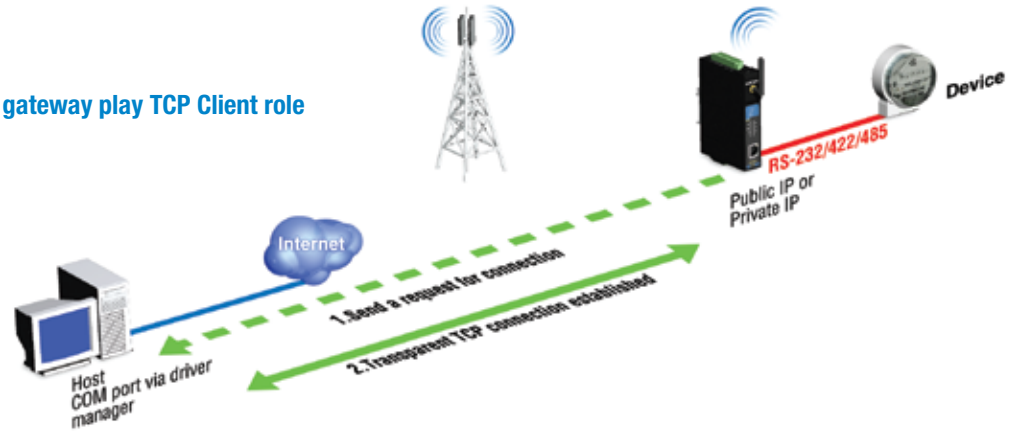
If your application involves a socket-based TCP server or TCP client, you can set your OnCell G3100 device to Socket Mode Socket operation mode by simply using the OnCell web console. You do not need to install any additional utilities onto the host PC but the socket software on the host PC will need to set up a socket connection with the OnCell G3100. The IP address of the SIM card on the OnCell G3100 device will determine the role of socket connection.

OnCell Device's IP Address	Suitable Role	Socket Mode Selection
Public address	Server role, Client role	TCP Server, TCP Client
Private IP address Like 10.x.y.x or 172.xx……	Client role	TCP Client

If both the host PC (at the control center) and the OnCell G3100 device have private IP addresses, you can use OnCell Central Manager on the OnCell G3100 to resolve the private IP to private IP problem and select TCP Server for the OnCell G3100's socket mode.

IP gateway play TCP Server role

IP gateway play TCP Client role



Short Message Connection (SMS Tunnel)

Short Message Service (SMS) is a very popular service offered by cellular providers. You can send and receive serial data via SMS by setting up the OnCell G3100 device's SMS Tunnel Mode.

The OnCell G3100's SMS Tunnel Mode uses a serial port to serial port communication tunnel to send SMS messages. There are 3 key inputs involved in transmitting SMS serial data.

1.Target phone number of the mobile device that will receive transmitted data
2.Pre-approved recipient phone numbers; unapproved numbers will be filtered out
3.Data format (i.e., ASCII, binary, UCS2)

Unlike GPRS and CSD, SMS employs a "store and forward" mechanism so messages are not transmitted in real time.

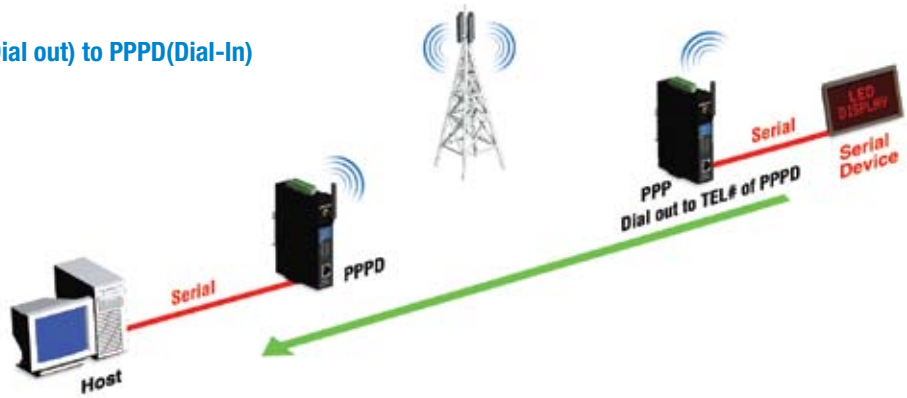
IP Gateways and CSD

Some cellular providers offer Circuit Switch Data (CSD) service, which transmits data over voice channels that are always connected, such as fax and modem service. However, CSD calls always occupy the phone which means you will still be charged for service even when you are not sending data. In additional, data throughput is limited and takes up too many resources. As a result, cellular providers usually do not offer CSD and the service is no longer offered in some countries. At the same time, 2G service is also being phased out in favor of 3G technologies. Check with your cellular provider to see if they offer these services.

The OnCell G3100 IP gateway can send IP stacks using PPP (Point to Point Protocol) capability over CSD service. There are 2 mechanisms for setting up your PPP connection:

1. The originating OnCell device (PPP) dials the terminating OnCell device (PPPD).

PPP(Dial out) to PPPD(Dial-In)



2.The originating OnCell device dials the phone number of the ISP (Internet Service Provider) just like an analog modem. Normally, ISPs offer free accounts and passwords for you to access the Internet.

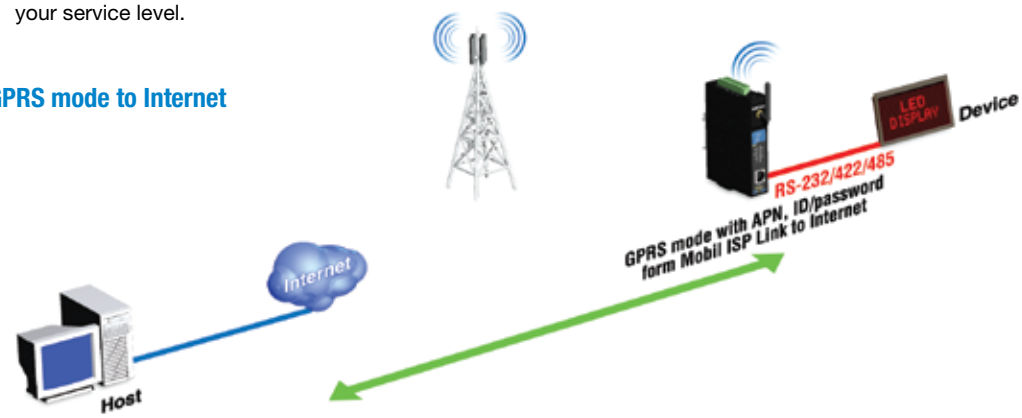
PPP to Internet via ISP

IP Gateways and GPRS

GPRS is designed for packet data communication and provides GSM users with access to the Internet from a cellular network. Before activating the GPRS function on your OnCell G3100, make sure that the SIM card is GPRS-enabled with the right APN string.

In order to activate GPRS service on your OnCell device, your SIM card must first be connected to a GSM network. That is why the GSM LED on your OnCell device will be lit for a while before the GPRS LED turns on. You will also need the APN (Access Point Name) and account password (not required by some cellular providers). The APN is a string that determines which Internet gateway (GGSN) from the cellular provider's network you can access. This may affect the IP address and services, such as port blocking and VPN, you are able to obtain from your provider. Cellular providers also maintain a database (HLR) to record and bill your service level.

GPRS mode to Internet



If your SIM card is already GPRS-enabled and has the right APN, then your OnCell G3100 will automatically set up the IP link for your application whether you're using socket mode or operation mode.

Modem Extension Mode (Virtual Modem)

Modem Extension Mode is a solution for

- Extending the distance from the control center to a pure AT modem, and
- Sending pure AT commands to control your OnCell G3100 device via Ethernet (longer distance).

If you need to control your modem from a longer distance, consider using an Ethernet link. This solution allows you to keep the serial control interface at the control center and send AT commands from the control center to your OnCell G3100 device by Ethernet.

You will first need to install OnCell Driver Manager on the controller side to create a virtual COM port, which will allow you to control the serial port as if it were a traditional modem and send AT commands to set up CSD calls, send SMS messages, or link to GPRS. You also can install the OnCell modem driver so you can set up dial up networking for your laptop.

3.5 How to Connect Ethernet Devices to Cellular Networks

Traditionally, Ethernet-based devices can only establish TCP/IP connections through wired LAN lines. At best, you may be able to deploy a WLAN environment to communicate with Ethernet devices in the field. A WLAN system can eliminate wires and cabling problems when installing and operating the devices. It also provides greater mobility, especially when the Ethernet devices are moving. When it comes to range, however, WLAN systems are still limited to local area networks and places with hardwire Internet connections.

What if Ethernet devices could be accessed through a cellular network? This would allow Ethernet devices to be accessible almost anywhere as long as cellular coverage is available. Ethernet to cellular technology can also provide primary and backup network connectivity. Moxa offers an easy and cost-effective means of connecting virtually any remote location or device to a corporate IP network. It is ideal for applications where wired networks (e.g., lease line / frame relay, CSU/DSU, fractional T1) are not feasible or where alternative network connections are required.

From WAN to LAN (TCP Server)

In this case, the Ethernet device, when acting as a server, is to be reached from the public domain. The TCP Server may be an industrial PC server, an I/O device with LAN interface, or any Ethernet routing device. As long as the device uses a LAN interface running on TCP protocols (even MODBUS TCP), the device can be reached. There may even be multiple Ethernet devices with different IP addresses connected to the IP gateway.

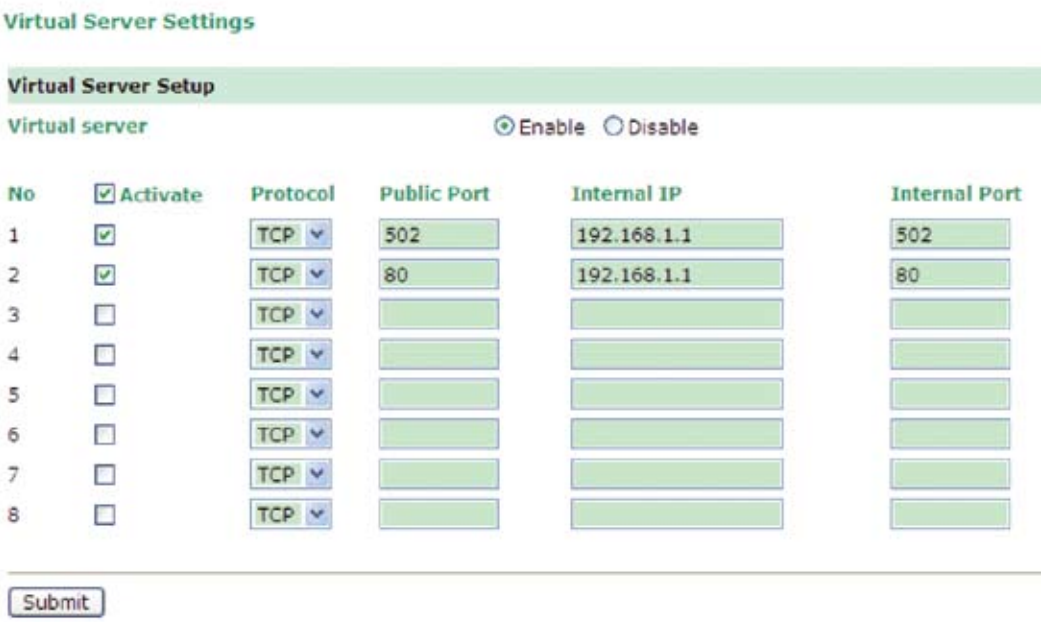
When a TCP Client device attempts to connect to the TCP Server, it will first need to make a TCP connection with the IP modem (OnCell), and then have the OnCell port forward the synchronization request to the TCP Server connected to it. Basically, the OnCell plays the role of a virtual server to allow clients to make a direct TCP connection to it before forwarding traffic to the actual server. Much like a WLAN router, the traffic from the WAN port is directed to the devices connected to the LAN port of the router.

It is important to note that your OnCell device will need to obtain a public WAN IP address from your cellular provider in order for it to be visible to the public domain. Private IP addresses are hidden from the public Internet so TCP Clients will not be able to find it on a public network. The WAN IP address of your OnCell device may be static or dynamic, but it must be a public IP address. If the public WAN IP address is a dynamic IP address (changes every time the OnCell reconnects to the cellular network), a useful function is to enable to DDNS (Dynamic DNS). DDNS allows the TCP clients to access the OnCell device by domain name. So even as the OnCell device's WAN IP address changes, the changed IP addresses continue to map to the same domain name through DDNS updates.

In cases where only private IP addresses are available from the cellular provider, the OnCell can still play the server role by enabling the OnCell Central Manager (see section 3.2 for details) function proprietary to Moxa's IP gateways.

How to configure the OnCell device as a virtual server

In the OnCell device's web console, you will find a virtual server settings page where you can set up multiple Ethernet devices connected to the OnCell device:



As you can see, virtual server setting is basically setting the forwarding ports. For example, you select an available public port that the OnCell's WAN IP will be listening on. A TCP client device will connect directly to the OnCell's WAN IP/Public Port when making a TCP connection with the server. Next, enter the actual server's IP address (Internal IP) to allow the OnCell to locate the server in the local network. An internal port (listening port on the actual server) is then specified so that the traffic coming through from the public port will be forwarded to the internal port. Lastly, you'll notice that both TCP and UDP traffic can be forwarded by the virtual server.

The previously mentioned DDNS function can be enabled on the OnCell device to compensate for dynamic WAN IP addresses:

From LAN to WAN

We now switch the role of the Ethernet device from TCP Server to TCP Client:

Now the OnCell device is a gateway for the TCP Client to route its traffic to the public domain through the cellular network. The NAT function built into the OnCell device allows the WAN and LAN interfaces to direct traffic to each other. The Ethernet device can now locate the server on the public domain to establish a remote connection. For example, multiple Ethernet devices at a remote site can act as TCP clients and all connect to the same server in the control center for central management.

When the OnCell is acting as a client, its WAN IP address will not be limited to public WAN IP addresses. The WAN IP address of the OnCell IP modem can be public or private, static or dynamic without any extra settings.

How to configure the OnCell as a gateway to the public domain

For the OnCell G3100 series, you do not need to perform extra settings to use the OnCell as a gateway for connected Ethernet devices to be able to access the public internet. The built-in NAT function is enabled by default, so by simply setting the default gateway IP address of the Ethernet device to the OnCell's LAN IP address, the Ethernet device will be able to connect to the Internet and initiate TCP connection requests to the TCP server.

Please note that if you are going to be accessing a domain name on the Internet, not only do you need to set the OnCell as your default gateway, but a public DNS server is also required for domain name access.

The OnCell can be both TCP Server and TCP Client

In some applications, Ethernet devices act in both the server and the client role. In these cases, the OnCell can play both roles as well. The virtual server settings and gateway settings can be used simultaneously in the same way a traditional router can forward traffic in both directions. As shown in the network diagram below, you only need two OnCell devices for two Ethernet devices to communicate with each other. The Ethernet devices do not need to be located in a hardwire Internet-ready area as long as there is a cellular signal present and the TCP Server/Client pair of the OnCell device can bridge a LAN connection.

3.6 How to Connect I/O Devices to Cellular Networks

SCADA Meets Ethernet

SCADA (Supervisory Control and Data Acquisition) is a computer-based industrial control system that plays an important role in the field of automation today. In particular, SCADA systems are used to monitor and control a process, including manufacturing, production, power generation, fabrication, refining, water treatment, distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, facility processes, and more. Some of the benefits provided by SCADA include:

- Setting up Communications for Data Acquisitions
- Graphics HMI
- Alarms
- Trends and Process Analyst
- Commands and Controls

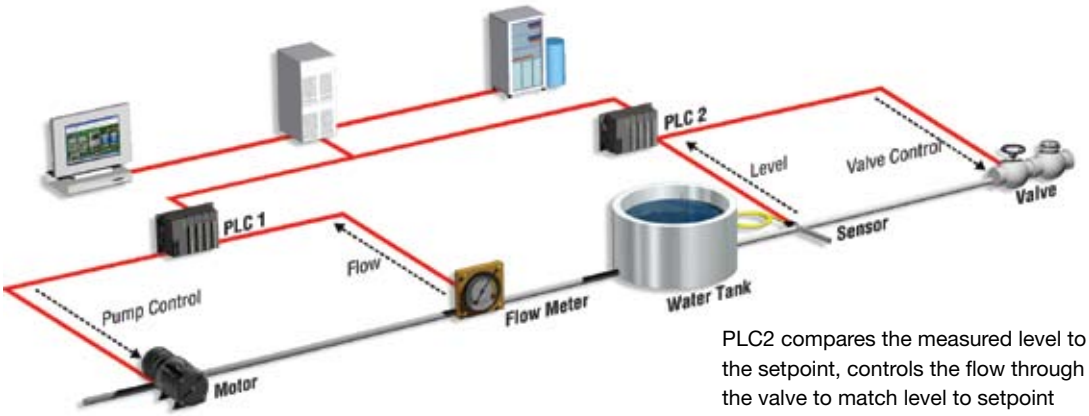
SCADA usually refers to centralized systems that monitor and control entire sites, or a network of systems spread out over large areas. Most control actions are performed automatically by intelligent I/O devices (i.e., Moxa's Active Ethernet I/O), remote terminal units (RTUs), or programmable logic controllers (PLCs). Host control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process, but the SCADA system may allow operators to change the setpoints for the flow, and enable alarm conditions, such as loss of flow and high temperature, to be displayed and recorded. The feedback control loop passes through the Active Ethernet I/O or RTU or PLC, while the SCADA system monitors the overall performance of the loop.

Modem Extension Mode (Virtual Modem)

Data acquisition begins at the RTU, PLC, or I/O device level, and includes meter readings and equipment status reports that are communicated to the SCADA system as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal I/O controls. An HMI is usually linked to the SCADA system's database and software programs, to provide trending, diagnostic data, and management information such as scheduled maintenance procedures, logistic information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides.

Data may also be fed to a commodity database to allow trending and other analytical auditing. SCADA systems typically implement a distributed database, commonly referred to as a tag database, which contains data elements called tags or points. A point represents a single input or output value monitored or controlled by the system. Points can be either "hard" or "soft". A hard point represents an actual input or output within the system, while a soft point results from logic and math operations applied to other points. (Most implementations conceptually remove the distinction by making every property a "soft" point expression, which may, in the simplest case, equal a single hard point.) Points are normally stored as value-timestamp pairs (a value and the timestamp when it was recorded or calculated). A series of value-timestamp pairs gives the history of that point. It's also common to store additional metadata with tags, such as the path to a field device or PLC register, design time comments, and alarm information.

The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs

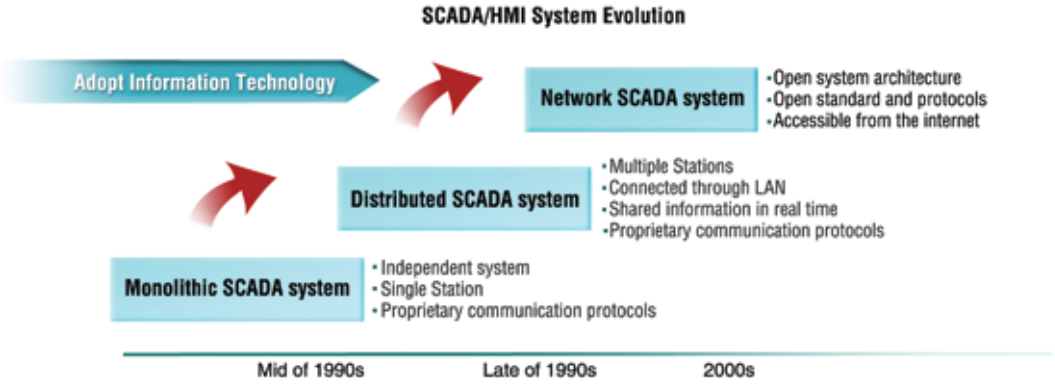


PLC2 compares the measured level to the setpoint, controls the flow through the valve to match level to setpoint

PLC1 compares the measured flow to the setpoint, controls the speed pump as required to match flow to setpoint

"Mix-and-Match" SCADA

SCADA/HMI systems evolved in three stages, including Monolithic, Distributed, and Network SCADA systems. Monolithic SCADA involves an independent system for single station and uses a vendor's proprietary communication protocols. As the number of monitoring sites increased, multiple stations were required for monitoring and control in a Distributed SCADA system. The introduction of LAN technology in the late 1990s provided SCADA systems with real-time monitoring capabilities. At the time, most communication protocols were proprietary.



Due to a limited choice of equipment when requirements changed, open communication protocols became increasingly popular, such as Modbus RTU and Modbus ASCII (originally both developed by Modicon) over RS-485. By 2000, most I/O makers offered completely open interfacing such as Modbus TCP over Ethernet and IP.

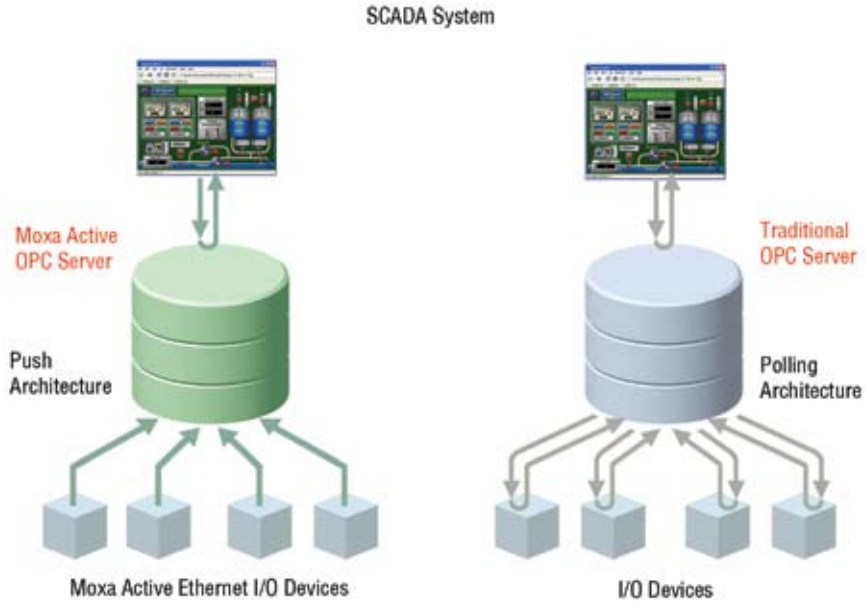
Today, Network SCADA systems, which use open system architecture, standards, and protocols, distribute functionality across a WAN rather than a LAN. It is now easier to connect third party peripheral devices because of the adoption of information technology. IT field protocols, such as Internet Protocol (IP), are used for communication between the master station and communications equipment. Due to the use of standard protocols, many Network SCADA systems are accessible from the Internet.
SCADA systems are coming in line with standard networking technologies. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. A key protocol is OPC Client/Server protocol.

Although it allows different equipment from different vendors to communicate with each other, it does not utilize the bi-directional and "push" technology advantages of Ethernet networks. For example, if an intelligent device wanted to send alarms and execute front-end logic, it could take advantage of Ethernet network communication technology used in IT. The vast majority of markets have accepted Ethernet networks for their HMI/SCADA systems.

What does the future have in store? Experts foresee the next generation of SCADA to be a mix-and-match system that takes advantage of XML, web service, push, and other modern web technologies.

New Push Technology from Moxa Active OPC Server

Active OPC Server Lite is a software package provided by Moxa that operates as an OPC driver for an HMI or SCADA system. It offers seamless connection from Moxa's ioLogik series products to SCADA systems, including Wonderware, Citect, and iFix. Active OPC Server Lite meets the latest standard of OPC DA 3.0, which allows connections to various kinds of devices and host OPC machines.

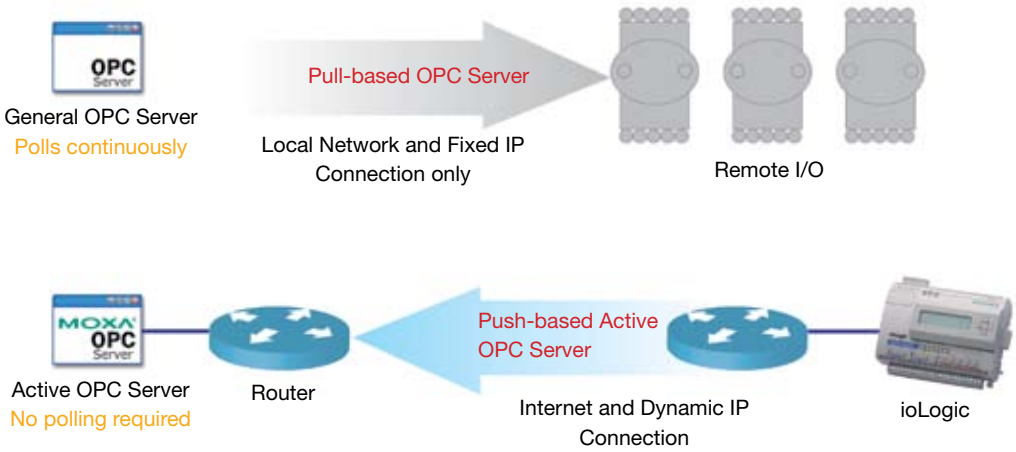


Communication from I/O to SCADA

There are many kinds of communication methods between SCADA/HMI software and remote devices, such as I/O devices, RTUs, or PLCs. In the past, proprietary protocols were provided by device manufacturers who always supplied drivers to make their devices compatible with SCADA/HMI software or provided their own SCADA software. Today, Modbus protocol is quickly becoming the standard among hardware manufacturers with SCADA/HMI software vendors also jumping on the wagon. Although Modbus offers compatibility between most devices and SCADA software, not all devices support Modbus protocol. Achieving a standard mechanism for communicating with numerous data sources, such as devices on the factory floor or a database in a control room, is the motivation for the development of OPC. SNMP protocol is used in IT to manage various Ethernet devices, and OPC Client/Server architecture supports SNMP. Moxa's innovative Active Ethernet I/O products support Modbus/TCP, OPC Client/Server, and SNMP for greater flexibility compared to passive remote I/O.

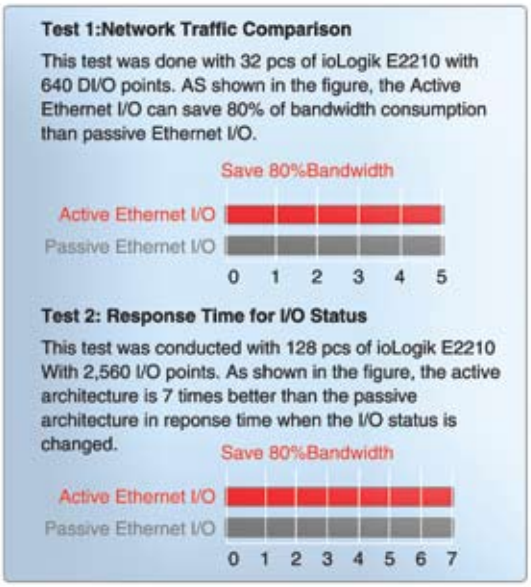
	Passive I/O	Active Ethernet I/O	RTU	PLC
Proprietary Protocol	No	No	No	Yes
Modbus/TCP	Yes	Yes	Yes	Yes
SNMP	No	Yes	No	No
OPC Client/Server (Polling)	No	Yes	No	Needs driver
OPC Client/Server (Push)	No	Yes	No	No

General OPC servers typically use the “poll/response,” or so-called “pull” architecture, to connect to Ethernet I/O devices, which involves an HMI/SCADA system continuously sending out commands to collect relevant data. Moxa’s Active OPC Server, with its non-polling architecture, supports the standard OPC protocol, but also offers active (or “push”) communication with Moxa’s ioLogik series of Active Ethernet I/O products to HMI/SCADA systems, providing instant I/O status reports.



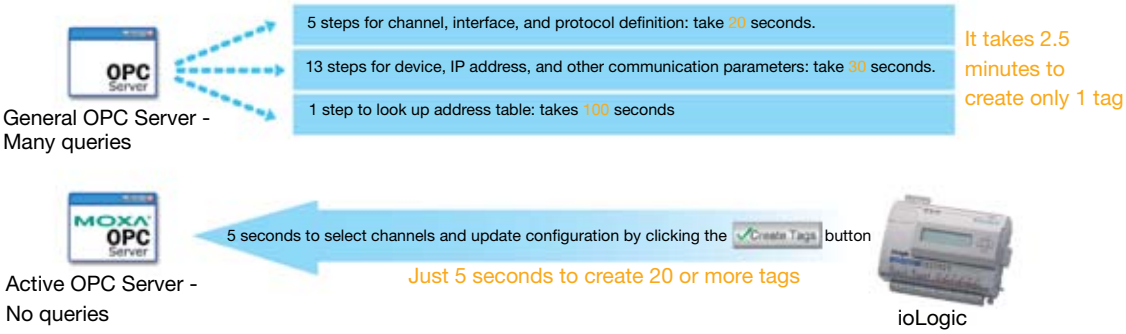
I/O Response that’s 7 Times Faster and Provides 80% off Bandwidth Usage with Event-driven Tag Updates

Adding additional I/O channels will tend to bog down an HMI/SCADA system’s operation, resulting in a longer response time , and high network bandwidth occupation, all because of the traditional “pull” architecture. Active tags created by Active OPC Server Lite and ioLogik series products report the I/O status only when it changes.This type of event-driven tag status update results in an I/O response time that is 7 times faster than other OPC Server packages (using a testing environment with 2,560 I/O channels). In a different test of network bandwidth usage, Active OPC Server Lite and the ioLogik caused an apparent 80% reduction in network traffic. The end result is that I/O access is more precise, and the cost of communicating with remote I/O devices is substantially lower, especially when the remote site has limited bandwidth (e.g., satellite, microwave, and cellular communication). At the same time, the CPU usage of the SCADA/HMI system is also reduced by 35% with this innovative push-based architecture, so that less maintenance effort and lower level hardware devices can be implemented.


Test 1:Network Traffic Comparison
This test was done with 32 pcs of ioLogik E2210 with 640 DI/O points. AS shown in the figure, the Active Ethernet I/O can save 80% of bandwidth consumption than passive Ethernet I/O.
Save 80%Bandwidth
Active Ethernet I/O
Passive Ethernet I/O
0 1 2 3 4 5
Test 2: Response Time for I/O Status
This test was conducted with 128 pcs of ioLogik E2210 With 2,560 I/O points. As shown in the figure, the active architecture is 7 times better than the passive architecture in reponse time when the I/O status is changed.
Save 80%Bandwidth
Active Ethernet I/O
Passive Ethernet I/O
0 1 2 3 4 5 6 7

Automatic Tag Generation

Active OPC Server Lite and ioLogik series products support “Auto Tag Generation,” which eliminates the headache of specifying target IP addresses, I/O channels, and data formats one by one, or editing and importing configuration text files, since Active OPC Server Lite creates the tags for the target ioLogik automatically. Simply select the channels that you need to update, and the tags are generated and configured automatically. Generally speaking, tag generation is 50 times faster with Active OPC Server Lite than with traditional OPC server packages. One of the biggest payoffs is that users will no longer need to be trained to install and configure your OPC.


OPC Server
5 steps for channel, interface, and protocol definition: take 20 seconds.
13 steps for device, IP address, and other communication parameters: take 30 seconds.
1 step to look up address table: takes 100 seconds
It takes 2.5 minutes to create only 1 tag
General OPC Server - Many queries
MOXA OPC Server
5 seconds to select channels and update configuration by clicking the Create Tags button
Just 5 seconds to create 20 or more tags
Active OPC Server - No queries
ioLogic

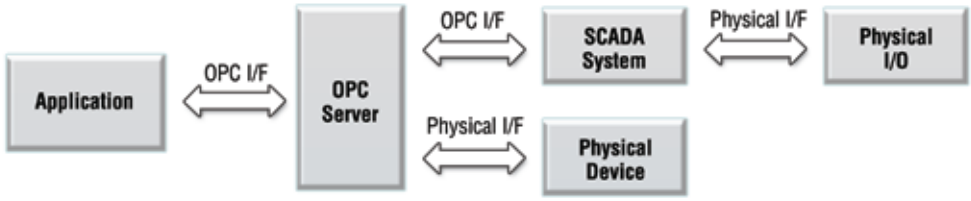
Dynamic IP/WAN Connection

Unlike the fixed IP requirements of Ethernet I/O with a traditional OPC server, Active OPC Server Lite and ioLogik products provide the flexibility of configuring the ioLogik to use dynamic IP addresses. The ioLogik connects directly to the Active OPC Server Lite instead of being polled, which makes dynamic IP addressing and WAN Access to the Ethernet I/O device possible, and adds even greater flexibility by allowing connections across firewalls. I/O devices for traditional data acquisition applications are not capable of using this approach.

OPC Fundamentals

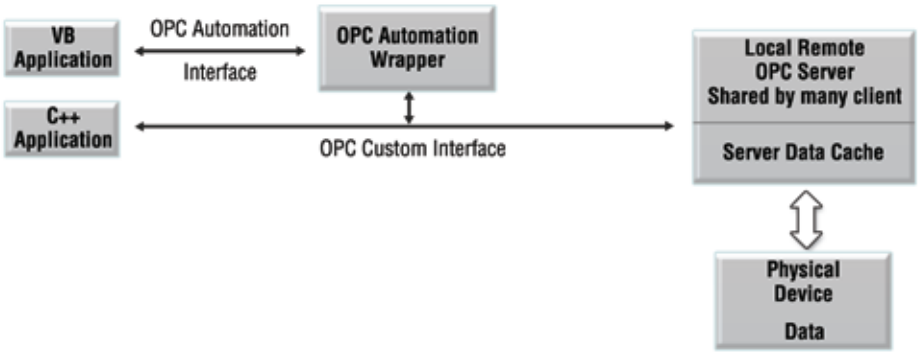
OPC (OLE for Process Control) is an industry standard created by the collaboration of a number of leading worldwide automation hardware and software suppliers, working in cooperation with Microsoft. The standard defines methods for exchanging real-time automation data between PC-based clients using Microsoft operating systems. “The OPC Specification is a non-proprietary technical specification that defines a set of standard interfaces based upon Microsoft’s OLE/COM/DCOM platform and .NET technology. The application of the OPC standard interface makes possible interoperability between automation/control applications, field systems/devices and business/office applications. Traditionally, each software or application developer was required to write a custom interface, or server/driver, to exchange data with hardware field devices. OPC eliminates this requirement by defining a common, high performance interface that permits this work to be done once, and then easily reused by HMI/SCADA, control and custom applications.

OPC simplifies system integration in a heterogeneous computing environment. However, functions such as security, batch and historical alarm, and event data access belong to the features that are addressed. OPC interfaces can be used in many places within an application. At the lowest level they can get raw data from the physical devices in a SCADA/HMI system, or from the SCADA/HMI system in the application. The architecture and design makes it possible to construct an OPC Server that allows a client application to access data from many OPC Servers provided by many different OPC vendors running on different nodes via a single object.



General OPC Architecture and Components

The architecture of OPC leverages the advantages of the COM interface, which provides a convenient mechanism to extend the functionality of OPC. OPC specifications always contain two sets of interfaces; Custom Interfaces and Automation interfaces.



The OPC Specification specifies the COM interfaces but not the implementation. It specifies the behavior that the interfaces are expected to provide to the client applications that use them. Like all COM implementations, the architecture of OPC is a client-server model where the OPC Server component provides an interface to the OPC objects and manages them. There are several unique considerations in implementing an OPC Server. The main issue is the frequency of data transfer over non-sharable communications paths to physical devices or other databases. Thus, we expect that OPC Servers will either be a local or remote EXE which includes code that is responsible for efficient data collection from a physical device or a database. An OPC client application communicates to an OPC server through the specified custom and automation interfaces. OPC servers must implement the custom interface, and optionally may implement the automation interface. In some cases the OPC Foundation provides a standard automation interface wrapper. This “wrapperDLL” can be used for any vendor-specific custom-server.

OPC Servers now register with the system via Component Categories. This allows the Microsoft ICatInformation (IID_ICatInformation) Interface on the StdComponentCatagoriesMgr (CLSID_ StdComponentCategoriesMgr) to be used to determine which OPC servers are installed on the local machine. The problem is that this does not work for remote machines because the Component Categories Manager is a DLL and the ICatInformation interface only works in-process. As a result, there is no easy way for a Client (including the Foundation supplied Automation Wrappers) to obtain a list of OPC Servers installed on a remote machine. The OPC Foundation supplied Server Browser OPCENUM.EXE can reside on any machine, will access the local Component Categories Manager, and provide a new interface IOPCServerList that can be marshaled and used by remote clients. This server has a published classid (see below) and can be installed once on any machine which hosts OPC servers. The client still needs to know the nodename of the target machine however he can now create this object remotely and use its IOPCServerList interface to determine what types and brands of servers are available on that machine.

OPC and DCOM: 5 Things You Need to Know

OPC technology relies on Microsoft's COM and DCOM to exchange data between automation hardware and software; however it can be frustrating for new users to configure DCOM properly. If you have ever been unable to establish an OPC connection or transfer OPC data successfully, the underlying issue is likely DCOM-related. In the following, we will discuss the steps necessary to get DCOM working properly and securely. A simple and effective strategy to establish reliable DCOM communication involves the following steps:

Remove Windows Security

The first step to establish DCOM communication is to disable the Windows Firewall, which is turned on by default in Windows XP Service Pack 2 and later. The Firewall helps protect computers from unauthorized access (usually from viruses, worms, and people with malicious or negligent intents). If the computer resides on a safe network, there is usually little potential for damage as long as the Firewall is turned off for a short period of time. Check with the Network Administrator to ensure it is safe to turn off the Firewall temporarily.

Set Up Mutual User Account Recognition

To enable both computers to properly recognize User Accounts, it is necessary to ensure that User Accounts are recognized on both the OPC Client and Server computers. This includes all the User Accounts that will require OPC access. If there are no User Accounts or Passwords already on the computers, please add them to both computers.

Configure System-wide DCOM Settings

OPC specifications depend on Microsoft's DCOM for the data transportation. Consequently, you must configure DCOM settings properly. It is possible to configure the default system-wide DCOM settings, as well for a specific OPC server. The system-wide changes affect all Windows applications that use DCOM, including OPC application. In addition, since OPC Client applications do not have their own DCOM settings, they are affected by changes to the default DCOM configuration. OPC communication only requires "Connection-Oriented TCP/IP", so add "Anonymous Logon" (required for OPCEnum) and "Everyone" to the list of "Group or user names" in each tab.

Configure Server Specific DCOM Settings

Once the system-wide DCOM settings are properly configured, turn attention to the server-specific DCOM settings. In the OPC-Server specific settings, only the Identity tab needs to change from the default settings. After opening the DCOM setting windows, find the OPC Server to configure and right-click on it. Select the Properties option in the list of objects in the right window pane. Choice the The system account (services only). The OPC Server will take the identity of the Operating System (or System for short). This is typically the desired setting for the OPC Server as the System Account is recognized by all computers on the Workgroup or Domain. In addition, no one needs to be logged on the computer, so the OPC Server can execute in an unattended environment. Disable this option if the OPC Server is not setup to execute as a Windows Service. If this is the case, simply configure the OPC Server to execute as a service before configuring this setting.

Restore Windows Security

Once you establish the OPC Client/Server communication, it is important to secure the computers again. This includes (but is not limited to):

a. Turn on the Windows Firewall again. This will block all unauthorized network traffic. You will also need to provide exceptions on two main levels:
   - Application level: specify which applications are able to respond to unsolicited requests.
   - Port-and-protocol level: specify that the firewall should allow or deny traffic on a specific port for either TCP or UDP traffic.

b. Modify the Access Control Lists (ACLs) to allow and deny the required User Accounts. This can be accomplished either through the system-wide settings of DCOMCNFG, or in the server-specific settings. Remember that OPCEnum requires the "Anonymous Logon" access. You may wish to remove this access. The consequence of this action will simply be that OPC Users will be unable to browse for OPC Servers on the specific computer where Anonymous Logon access is not available. However, users will indeed be able to properly connect to and exchange data with the OPC Server.

We encourage you to complete your DCOM setup with this step. Integrators frequently establish OPC communication and don't spend the necessary time to secure the computers again. This can lead to catastrophic results if network security is compromised due to a virus, worm, malicious intent, or simply unauthorized "experimentation" by well-meaning coworkers.

For more detail information, please refer to the OPC Training Institute: http://www.opcti.com

Enhance OPC Capability for Cellular Communications

GPRS is a communication technology that allows data acquisition systems to overcome the difficulty of cabling for wide area remote sites. GPRS applications are becoming more and more prevalent due to the ease with which they can be implemented, but the dynamic IP address issues associated with GPRS networking continue to frustrate system integrators. The fact that most GPRS devices use dynamic IP addresses can be somewhat frustrating. What this means is that telecom service providers (commonly referred to as carriers) often assign temporary IP addresses to their clients to access the Internet. Compared with static IP addresses, using dynamic IP addresses make it difficult for the control centers to keep in constant contact with remote devices.

The Traditional Polling Architecture of GPRS Networks

Traditional monitoring and alarm systems use a polling architecture that will only work properly if the host knows the IP addresses of the I/O devices used by the system. The trouble with I/O devices with GPRS capability is that the devices receive a different IP address every time they connect to the GPRS network. Three distinct solutions have been developed to tackle this obstacle:

Solution 1: Public Static IP Address

The first choice is to get a public static IP address; some carriers can assign a static IP address to a specific SIM card. This way, all the I/O devices will have their own static IP address and the entire system will operate in the same manner as a traditional monitoring system that uses physical wiring. Perhaps the main benefit of this solution is that it behaves the same as a wired solution. However, not all carriers offer this kind of service, and when they do the cost is relatively high.

Solution 2: VPN Service Provided by Carrier/MVNO

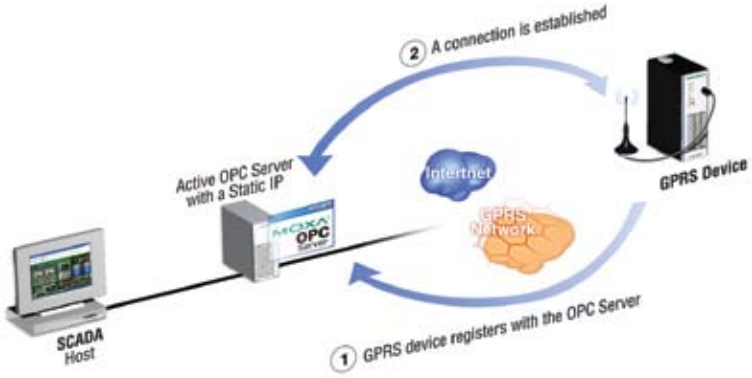
A VPN (Virtual Private Network) is a secure LAN solution that groups specific devices together. VPN has two major functions—security and grouping—and for the GPRS world the VPN grouping concept solves the dynamic IP address issues. The grouping of the devices into one private network prevents unauthorized persons from accessing the data. For this VPN solution, customers are required to buy a number of different GPRS on-line services, and to apply for access to a Virtual Private Network (VPN). When the GPRS device dials up, the carrier will assign a private IP address to it and because the private IP address is on the same network segment as the host, the host and devices can maintain bi-directional communication using a polling architecture.

Solution 3: DDNS

Using dynamic IP addresses is often necessary since many ISPs do not provide static IP addresses, or because the cost of obtaining a static IP address is too expensive. The Dynamic Domain Name System (DDNS) is used to convert a device's name into a dynamic IP address so that remote devices can communicate with the control center using a fixed domain name. When GPRS devices get an IP from the carrier, they will automatically connect to the GPRS network. Each time a GPRS device's built-in DDNS client gets a new IP address, it will send the IP address to the DDNS sever. The mapping table in the DDNS server is refreshed each time the DDNS receives a new IP address from the devices.

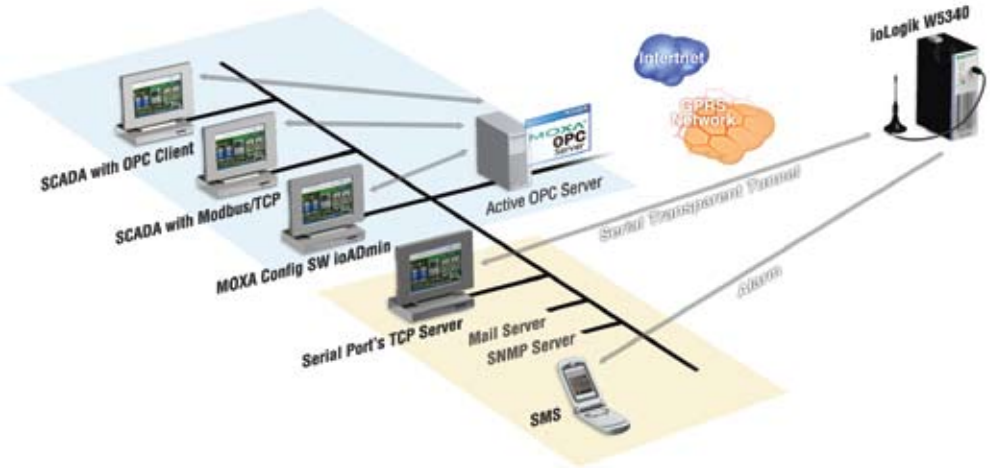
New Push Architecture for GPRS Networks

Push Architecture is a mobile centric solution. Service providers such as web portals and e-mail servers use a fixed domain name. Clients such as mobile phones get information from these service providers by "pushing" the connection request to the Web and e-mail servers, and when a connection is established, the communication is bi-directional. Unlike the so-called polling architecture, push technology makes bi-directional communication possible for GPRS networks that are using either a dynamic or a static IP address. A remote device with front-end intelligence can report its I/O status to the host and connect to the GPRS network when it needs to. Since Moxa's Active OPC Server supports push technology, our GPRS I/O family of products creates a software-based gateway that makes communications easier. By using a static IP address on the Active OPC Server, the GPRS I/O device can connect to the GPRS network and Active OPC Server without needing to worry about the IP address issues. The topology is described below:



Compared with polling architecture, push technology not only solves the IP address issues but also reduces network loading as well as bandwidth consumption.
Moxa's ioLogik W5340 Active GPRS I/Os takes full advantage of all the benefits of push technology and Active OPC Server. What Active GPRS I/O and Active OPC Server provide are:

1. SCADA Data Acquisition by OPC protocol.
2. SCADA Data Acquisition by Modbus/TCP protocol.
3. ioAdmin.exe: active GPRS I/O's configuration software.



Alarm messages, such as e-mail and SNMP trap or user definable TCP/UDP raw packets, can all be actively pushed to e-mail servers, SNMP trap servers, or TCP/UDP servers. SMS can be pushed from the Active GPRS I/O to an engineer's cellular phone.

Active OPC server is an exceptionally powerful gateway for Active GPRS I/O and plays the role of managing IP addresses, GPRS I/O device names, data acquisition gateways, and configuration gateways. This is truly the easiest solution for the GPRS industry to eliminate IP address and communication problems.

Benefits of Using Active GPRS I/O

Moxa's W5340 Active GPRS I/O devices come equipped with 4 analog inputs, 8 software configurable DI/Os, and 2 relay outputs. In addition, the built-in GPRS communication, front-end intelligence, and data logging function give users the advantage of a highly integrated solution. The W5340 also features a 3-in-1 serial port (RS-232/422/485) for connecting field serial devices such as instruments or meters. The benefits of using Active GPRS I/O include:

- A cost-effective solution for GPRS telemetry applications.
- The best choice for solving the dynamic IP issue: whether the IP is public or private, dynamic or static.
- Easy installation: with Active OPC's support, the W5340 can push IP addresses and I/O status to Active OPC server.
- Flexible Event Handling thanks to the Click&Go logic inside.
- Rich Alarm functions: SMS, SNMP trap, and e-mail.
- Lower bandwidth consumption: push architecture reduces bandwidth by 80% compared to the polling architecture.
- Faster response time because of push technology and event handling
- Data Logging: Local data logged to SD card and pushed to host by TFTP.

Conclusion

Remote monitoring and alarm systems used in water distribution, pipeline management, and environmental monitoring applications must be capable of covering a wide area and function reliably. Most importantly, the cost must be affordable. A remote monitoring and alarm solution with Moxa's Active GPRS I/O devices and Active OPC Server help users overcome the frustrations associated with using dynamic IP addresses, and makes it extremely easy to connect to SCADA systems.

Reference:

[1] http://en.wikipedia.org/wiki/SCADA

[2] http://www.citect.com/index.php?option=com_content&view=article&id=1502&Itemid=1366

[3] How to put SCADA on the Internet, http://www.controleng.com/article/CA321065.html

[4] OPC & DCOM: 5 Things You Need to Know, www.opcti.com

MOXA®

About Moxa

For more than twenty years, industrial systems integrators have relied on Moxa products in major device networking installations around the world. Moxa offers industrial-grade solutions backed by an excellent warranty and highly-specialized technical support for a diverse range of applications, including connecting PLCs to a wireless control network, transmitting temperature signals over long distances, and automating device control monitoring at remote locations.

Warranty 5 Year

Moxa Inc.
www.moxa.com
info@moxa.com

Moxa Americas
Toll-free: 1-888-MOXA-USA
(1-888-669-2872)
Tel: +1-714-528-6777
Fax: +1-714-528-6778
www.moxa.com
usa@moxa.com

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99
www.moxa.com
europe@moxa.com

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231
www.moxa.com
asia@moxa.com

Moxa China
Shanghai Office
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505
www.moxa.com.cn
china@moxa.com

Beijing Office
Tel: +86-10-6872-3959/60/61
Fax: +86-10-6872-3958
www.moxa.com.cn
China@moxa.com

Shenzhen Office
Tel: +86-755-8368-4084/94
Fax: +86-755-8368-4148
www.moxa.com.cn
china@moxa.com

©2009 Moxa Inc. All rights reserved.
The MOXA logo is a registered trademark of Moxa Inc. All other logos appearing in this document are the intellectual property of the respective company, product, or organization associated with the logo.

Trademark Credits
The Moxa Inc. logo is a registered trademark of Moxa Inc. All other trademarks mentioned in this document are the property of their respective owners.

P/N: 1900040901050